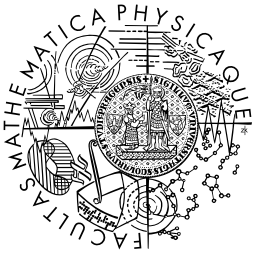


MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

DIPLOMOVÁ PRÁCA

Kristína Mišlanová

Kvaterniónové algebry a jednotky

Katedra algebry

Vedúci diplomovej práce: Mgr. Vítězslav Kala, Ph.D.
Študijný program: Matematika
Študijný odbor: Matematické štruktúry

Praha 2021

Prohlašuji, že jsem tuto diplomovou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Týmto by som sa chcela poďakovať svojmu vedúcemu Víťovi za všetky dôležité pripomienky, odbornú pomoc pri písaní práce, trpezlivosť pri riešení problémov a najmä za mimoriadne ochotný a priateľský prístup.

Názov práce: Kvaterniónové algebry a jednotky

Autor: Kristína Mišlanová

Katedra: Katedra algebry

Vedúci diplomovej práce: Mgr. Vítězslav Kala, Ph.D., Katedra algebry

Abstrakt: Cieľom tejto práce je štúdium hamiltonovských kvaterniónov $\mathbb{H}$ a kvaterniónových algebier. Prvé dve kapitoly sú založené na článku Quaternion algebras [5] od K. Conrada a zvyšok na knihe Quaternion algebras [11] od J. Voighta. Na začiatku sa venujeme vybudovaniu teórie ohľadom kvaterniónov, kvaterniónových algebier a študovaniu ekvivalentných podmienok pre určovanie rozštiepiteľných a nerozštiepiteľných kvaterniónových algebier. Následne, až na izomorfizmus, charakterizujeme kvaterniónové algebry nad niekoľkými rôznymi poľami, ako $\mathbb{R}$, $\mathbb{C}$ alebo $\mathbb{F}_p$. V tretej kapitole sa práca zameriava na rády v kvaterniónových algebrách, predovšetkým na Lipschitzov a Hurwitzov rád. Štvrtá kapitola je venovaná vzťahu medzi jednotkovými kvaterniónmi a rotáciami v $\mathbb{R}^3$, vďaka ktorému sa nám podarí charakterizovať konečné podgrupy $\mathbb{H}^1$ alebo aj $\mathbb{H}^\times$. Tento výsledok následne použijeme v poslednej kapitole, kde sa zameriame hlavne na problém charakterizácie grúp jednotiek v rádoch v hamiltonovských kvaterniónoch.

Kľúčové slová: hamiltonovské kvaternióny, kvaterniónové algebry, rády, grupy jednotiek

Title: Quaternion algebras and units

Author: Kristína Mišlanová

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Department of algebra

Abstract: The aim of this work is to study the Hamiltonian quaternions $\mathbb{H}$ and quaternion algebras. The first two chapters are based on the article Quaternion algebras [5] by K. Conrad and the rest on the book Quaternion algebras [11] by J. Voight. In the beginning, we mainly develop the theory about quaternions, quaternion algebras and study equivalent conditions for being a split or non-split quaternion algebra. After that, we also characterize, up to isomorphism, quaternion algebras over several fields such as $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{F}_p$. In the third chapter, the thesis deals with orders in quaternion algebras, especially Lipschitz and Hurwitz order. The fourth chapter is dedicated to the relationship between unit quaternions and rotations in $\mathbb{R}^3$, thanks to which we can characterize finite subgroups of $\mathbb{H}^1$, or equivalently $\mathbb{H}^\times$. This result will be used in the last chapter, where we are mainly focused on the problem of characterization of the group of units in orders in Hamiltonian quaternions.

Keywords: Hamiltonian quaternions, quaternion algebras, orders, groups of units

Obsah

Úvod

Pojem hamiltonovských kvaterniónov je v dnešnej dobe v matematike pomerne známy. Ak sa však pozrieme na začiatok, tak za svoj vznik vďačia ešte oveľa jednoduchšej štruktúre komplexných čísel. Práve tejto štruktúre sa pôvodne venoval William Rowan Hamilton. Úplne prvým kľúčovým krokom bolo, že sa na komplexné čísla pozeral ako na body v rovine, a teda ich popisoval dvojicou reálnych čísel a na základe toho definoval aj ich sčítanie a násobenie, ktoré vieme popísať geometrickými operáciami.

Prirodzeným ďalším krokom bola snaha rozšíriť tento koncept do priestoru, a teda na trojice reálnych čísel, kde by každé číslo pozostávalo z reálnej časti a dvoch rôznych imaginárnych častí. V tejto otázke bohužiaľ ani po rokoch úspešný nebol. Namiesto toho sa mu však v roku 1843 podarilo tento problém vyriešiť v dimenzii 4, kde zaviedol novú algebraickú štruktúru, v ktorej každé číslo pozostáva z reálnej časti a troch rôznych imaginárnych častí i, j a k. Pričom platí, že násobenie v tejto štruktúre nie je komutatívne, ale podlieha pravidlám $i^2 = j^2 = -1$, $k = ij = -ji$. Táto štruktúra je po svojom objaviteľovi dnes známa ako hamiltonovské kvaternióny a označujeme ju $\mathbb{H}$.

Následne sa opäť objavila otázka, či je možné štruktúru kvaterniónov ešte nejako zovšeobecniť. Naskytá sa hneď niekoľko možností. V kvaterniónoch je presne dané, že $i^2 = j^2 = -1$. No čo ak by konštanta -1 nebola fixne daná, ale mohli by sme len predpokladať, že $i^2 = a$, $j^2 = b$ pre nejaké a a b? Čo ak by sme nepracovali len nad poľom reálnych čísel? Práve na základe tejto variability vznikla definícia kvaterniónovej algebry $\left(\frac{a,b}{F}\right)$, ktorá prirodzene zovšeobecňuje kvaternióny.

V tomto bode narážame na prvý z cieľov tejto práce, ktorým bolo podrobne vybudovať teóriu ohľadom hamiltonovských kvaterniónov, ale aj kvaterniónových algebier, ktorým sa následne vo zvyšku práce budeme venovať. Prvá kapitola slúži hlavne na zhrnutie základných pojmov a vlastností týchto štruktúr.

V druhej kapitole sa pozrieme na izomorfizmus kvaterniónových algebier. Vo vete 2.7 ukážeme, že každá kvaterniónová algebra $\left(\frac{a,b}{F}\right)$ je buď rozštiepiteľná, a teda izomorfná algebre matíc $M_2(F)$, alebo je nerozštiepiteľná a predstavuje nekomutatívne pole. Následne vo vetách 2.8, 2.9 charakterizujeme ekvivalentné podmienky, za akých tieto prípady nastávajú. Na záver sa pozrieme na niektoré konkrétne polia a vo vetách 2.11, 2.12, 2.18 charakterizujeme až na izomorfizmus kvaterniónové algebry nad $\mathbb{R}, \mathbb{C}, \mathbb{F}_p$ a v 2.17 zhrnieme situáciu nad $\mathbb{Q}$. V týchto kapitolách budeme vychádzať predovšetkým z článku *Quaternion algebras, K. Conrad* [5], ktorý doplníme o niektoré vlastné dôkazy.

V tretej kapitole zadefinujeme rády v algebrách a zhrnieme niekoľko ich vlastností. Následne dôkladne rozoberieme tri príklady rádov v kvaterniónových algebrách, pričom opodstatnenosť ich voľby sa ukáže v ďalších kapitolách. Konkrétne sa jedná o Lipschitzov a Hurwitzov rád v $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ a o jeden rád v algebre $\left(\frac{-3,-1}{\mathbb{Q}}\right)$. Pri každom z rádov sme okrem ich definície a popisu prvkov uviedli aj to, ako vyzerá ich grupa jednotiek - tvrdenia 3.12, 3.15, 3.21, prípadne sme uviedli, aký je medzi nimi vzťah, respektíve že sú maximálnymi rádmi. Tu sa jedná o tvrdenia 3.16 a 3.20. Pri všetkých spomínaných sa jednalo často o vlastné dôkazy, alebo to boli podrobnejšie rozpracované dôkazy z *Quaternion algebras, J. Voight* [11].

V štvrtej kapitole sa naspäť vraciame ku štruktúre pôvodných hamiltonovských kvaterniónov a pozrieme sa na ich geometrickú interpretáciu. Aj keď to na prvý pohľad nemusí byť zrejmé, tak sa dá ukázať, že jednotkové hamiltonovské kvaternióny veľmi prirodzeným spôsobom popisujú rotácie v $\mathbb{R}^3$. Konkrétne vo vete 4.3 ukážeme, že každý kvaterniónový pár $\pm q \in \mathbb{H}^1$ jednoznačne určuje uhol a os rotácie v $\mathbb{R}^3$. Ako dôsledok tohto zistenia dostávame pre nás kľúčový izomorfizmus $\mathbb{H}^1/\{\pm 1\} \simeq SO(3)$. Pri tomto začiatku štvrtej kapitoly sme vychádzali z kníh *Quaternion algebras, J. Voight* [11] a *The four pillars of geometry, J. Stillwell* [10], pričom jednotlivé dôkazy sme detailne rozpracovali.

Problém konečných podgrúp grupy $SO(3)$ je dnes už veľmi známy, a preto sme si dovolili tento výsledok iba bez dôkazu zhrnúť vo vete 4.6. Dokázaný sa dá nájsť napríklad v článku *Classifying the finite subgroups of* $SO(3)$ [2]. Z tohto titulu nám bolo umožnené vyššie spomínaný izomorfizmus nazvať kľúčovým, keďže vďaka nemu vieme charakterizovať konečné podgrupy $\mathbb{H}^1/\{\pm 1\}$. Práve tejto otázke je venovaný zvyšok štvrtej kapitoly. V ňom sme si dovolili uviesť vlastné podrobné výpočty s tabuľkami a obrázkami, pomocou ktorých postupne charakterizujeme jednotlivé konečné podgrupy $\mathbb{H}^1/\{\pm 1\}$ v reči kvaterniónov, vďaka ich geometrickej interpretácií ako podgrúp $SO(3)$. Na záver vždy ešte každú z daných grúp pozdvihneme na konečnú podgrupu $\mathbb{H}^1$. Najdôležitejším výsledkom tejto kapitoly je teda veta 4.20, ktorá úplne charakterizuje konečné podgrupy $\mathbb{H}^1$, čo, ako ľahko ukážeme, je zároveň aj charakterizácia konečných podgrúp $\mathbb{H}^\times$. Na záver tejto kapitoly ešte pre úplnosť v sekcii 4.4 prehľadne zhrnieme prezentácie týchto jednotlivých podgrúp podľa knihy *Generators and Relations for Discrete Groups, H. S. M. Coxeter, W. O. J. Moser* [6].

V piatej kapitole sa dostávame ku druhému hlavnému cieľu tejto práce, ktorý ozrejmí celú našu cestu v niekoľkých predchádzajúcich kapitolách a jednotlivé výsledky spolu prepojí. Bude pozostávať z toho, že si vezmeme takú kvaterniónovú algebru $\left(\frac{a,b}{\mathbb{Q}}\right)$, že platí $\left(\frac{a,b}{\mathbb{R}}\right) \simeq \mathbb{H}$. Následne si v danej kvaterniónovej algebre vezmeme rád $\mathcal{O} \in \left(\frac{a,b}{\mathbb{Q}}\right)$. Potom sa prirodzene naskytá otázka, ako vyzerá grupa jednotiek v takomto ráde, a práve to v piatej kapitole vyriešime. Ukážeme, že každá takáto grupa jednotiek $\mathcal{O}^\times$ je konečnou podgrupou $\mathbb{H}^\times$, a teda na jej skúmanie môžeme využiť naše výsledky zo štvrtej kapitoly. Predtým ako sa k tomu dostaneme, však na začiatku piatej kapitoly ešte vybudujeme časť teórie ohľadom kvadratických polí, ktorú budeme využívať. V tejto časti sa budeme odkazovať na článok *Factoring in quadratic field, K. Conrad* [4] a knihu *A Classical Introduction to Modern Number Theory, K. Ireland a M. Rosen* [8].

Všetky naše úvahy v druhej polovici práce, a predovšetkým v piatej kapitole teda smerovali k výsledku, ktorý sme zhrnuli vo vete 5.17. Týmto výsledkom je úplná charakterizácia grúp jednotiek v rádoch v hamiltonovských kvaterniónoch. Pri dôkaze sme sa opierali o už zmienenú knihu *Quaternion algebras, J. Voight* [11], v ktorej je dôkaz naznačený. Naším cieľom a vlastným prínosom bolo v práci daný dôkaz v oveľa vyššej miere detailnejšie rozpracovať, doplniť a zároveň ho podložiť všetkými predchádzajúcimi výsledkami z tretej a štvrtej kapitoly, ktoré v danej knihe v takejto podobe chýbajú.

1. Kvaternióny a kvaterniónové algebry

Prvým z cieľov práce bude ucelene vybudovať základnú časť teórie ohľadom hamiltonovských kvaterniónov a ich následného zovšeobecnenia, ktoré predstavujú kvaterniónové algebry. Priamo v prvej kapitole sa s týmito štruktúrami zoznámime a zhrnieme si pojmy a vlastnosti, ktoré sa týkajú tejto problematiky, a na ktoré sa vo zvyšku práce budeme odkazovať. Väčšina týchto základných informácií sa dá nájsť napríklad v článku Quaternion algebras, K. Conrad [5], z ktorého budeme vychádzať.

1.1 Hamiltonovské kvaternióny

Na začiatok sa pozrieme na štruktúru samotných hamiltonovských kvaterniónov a uvedieme niekoľko kľúčových pojmov, ktoré s nimi súvisia. Pred tým, ako začneme, môžeme ešte podotknúť, že pri hamiltonovských kvaterniónoch vidno istú podobnosť s komplexnými číslami. Je tomu tak preto, lebo konštrukcia hamiltonovských kvaterniónov vznikla v roku 1843 práve ako snaha W. R. Hamiltona rozšíriť pojem komplexných čísel do vyššej dimenzie. Práve po ňom nesú aj svoje pomenovanie.

Definícia 1.1 (Hamiltonovské kvaternióny)**.** Hamiltonovské kvaternióny *definujeme ako nekomutatívny okruh* $\mathbb{H} = \{t + xi + yj + zk \mid t, x, y, z \in \mathbb{R}\}$ *spolu s nasledujúcimi podmienkami na násobenie:*

- $i^2 = j^2 = k^2 = -1$,
- $ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j$,
- *pre každé* $a \in \mathbb{R}$ *platí, že komutuje s* i, j *aj* k.

Poznámka. Každý hamiltonovský kvaternión $q = t + xi + yj + zk$ delíme na jeho reálnu časť, ktorú predstavuje t, a na imaginárnu časť $xi + yj + zk$. Pričom odteraz sa budeme niekedy na hamiltonovské kvaternióny odvolávať už iba ako na kvaternióny.

Definícia 1.2 (rýdzo imaginárny kvaternión)**.** Rýdzo imaginárny kvaternión *je kvaternión v tvare* $q = xi + yj + zk$*, teda kvaternión s nulovou reálnou časťou. Navyše definujeme* $\mathbb{H}^0 = \{q \in \mathbb{H} \mid q = xi + yj + zk\}$.

Poznámka. Priamo z definície $\mathbb{H}^0$ vidíme, že platí izomorfizmus $\mathbb{R}^3 \simeq \mathbb{H}^0$ ako izomorfizmus vektorových priestorov nad $\mathbb{R}$, keďže každý rýdzo imaginárny kvaternión $q = xi + yj + zk$ je vlastne popísaný trojicou reálnych čísel (x, y, z).

Príklad. Vyššie zadefinované pojmy si môžeme ilustrovať aj na príklade. Vezmime si dva kvaternióny $q_1 = i + 2j$, $q_2 = 3 + j + k$. Podľa definície 1.2 vidíme, že q_1 je rýdzo imaginárny kvaternión, zatiaľ čo q_2 má aj reálnu časť, ktorá je rovná 3, a imaginárnu časť rovnú $j + k$. Na štruktúre hamiltonovských kvaterniónov máme zadefinované aj operácie sčítania a násobenia. Pravidlá na násobenie sú súčasťou samotnej definície hamiltonovských kvaterniónov 1.1:

- $q_1 + q_2 = (i + 2j) + (3 + j + k) = 3 + i + 3j + k$,
- $q_1 q_2 = (i+2j)(3+j+k) = 3i+ij+ik+6j+2j^2+2jk = 3i+k-j+6j-2+2i = -2 + 5i + 5j + k$.

Definícia 1.3 (združený kvaternión)**.** *Nech $q \in \mathbb{H}$, $q = t + xi + yj + zk$. Potom definujeme k nemu* združený kvaternión *$\overline{q}$ ako $\overline{q} = t - xi - yj - zk$.*

Definícia 1.4 (norma kvaterniónov)**.** *Nech $q \in \mathbb{H}$, $q = t + xi + yj + zk$. Potom* normu kvaterniónu *q definujeme ako $N(q) = q\overline{q} = t^2 + x^2 + y^2 + z^2$.*

Už priamo z definície vidíme, že norma kvaterniónu bude vždy nezáporné reálne číslo, keďže sa jedná o súčet štyroch štvorcov reálnych čísel.

Príklad. Pre kvaternión $q = 3 + j$ je združený kvaternión $\overline{q} = 3 - j$, a teda jeho norma je $N(q) = q\overline{q} = (3 + j)(3 - j) = 3^2 - 3j + 3j - j^2 = 9 + 1 = 10$.

Tvrdenie 1.5 (multiplikativita normy kvaterniónov)**.** *Nech q_1, q_2 sú kvaternióny. Potom platí vzťah $\overline{q_1 q_2} = \overline{q_2} \cdot \overline{q_1}$, z čoho plynie $N(q_1 q_2) = N(q_1)N(q_2)$.*

Dôkaz. Vlastnosť $\overline{q_1 q_2} = \overline{q_2} \cdot \overline{q_1}$ vieme overiť priamym roznásobením oboch strán:

$$\begin{aligned}
\overline{q_1 q_2} =& \overline{(t_1 + x_1 i + y_1 j + z_1 k)(t_2 + x_2 i + y_2 j + z_2 k)} \\
=& t_1 t_2 - t_1 x_2 i - t_1 y_2 j - t_1 z_2 k - x_1 t_2 i - x_1 x_2 - x_1 y_2 k + x_1 z_2 j - y_1 t_2 j + \\
& y_1 x_2 k - y_1 y_2 - y_1 z_2 i - z_1 t_2 k - z_1 x_2 j + z_1 y_2 i - z_1 z_2 \\
=& (t_2 - x_2 i - y_2 j - z_2 k)(t_1 - x_1 i - y_1 j - z_1 k) \\
=& \overline{(t_2 + x_2 i + y_2 j + z_2 k)}\ \overline{(t_1 + x_1 i + y_1 j + z_1 k)} = \overline{q_2} \cdot \overline{q_1}
\end{aligned}$$

Ako dôsledok dostávame:

$$N(q_1 q_2) = q_1 q_2 \overline{q_1 q_2} = q_1 q_2 \overline{q_2}\ \overline{q_1} = q_1 N(q_2) \overline{q_1} = q_1 \overline{q_1} N(q_2) = N(q_1)N(q_2).$$

□

Definícia 1.6 (jednotkový kvaternión)**.** *Nech $q \in \mathbb{H}$. Potom q je* jednotkový kvaternión*, ak platí $N(q) = 1$. Ďalej definujeme $\mathbb{H}^1 = \{q \in \mathbb{H} \mid N(q) = 1\} = \{t + xi + yj + zk \in \mathbb{H} \mid t^2 + x^2 + y^2 + z^2 = 1\}$.*

Tvrdenie 1.7 (inverzný kvaternión)**.** *Nech $q \in \mathbb{H}$, $q \neq 0$. Potom k nemu existuje z oboch strán inverzný kvaternión a je rovný $q^{-1} = \overline{q}/N(q)$.*

Dôkaz. Pre $q \neq 0$ platí, že $N(q) > 0$, takže môžeme využiť vzťah pre normu $N(q) = q\overline{q} = \overline{q}q$. Odkiaľ priamo plynie $q^{-1} = \overline{q}/N(q)$.

□

Keďže každý nenulový prvok má inverz, tak môžeme písať, že grupu jednotiek tvorí $\mathbb{H}^\times = \mathbb{H} \setminus \{0\}$. Z toho priamo dostávame nasledujúcu vetu.

Veta 1.8. *Hamiltonovské kvaternióny tvoria nekomutatívne pole*[1]*.*

Príklad. Z minulého príkladu vieme, že pre $q = 3 + j$ máme združený kvaternión $\overline{q} = 3 - j$ a navyše $N(q) = 10$. To znamená, že k nemu inverzný kvaternión bude $q^{-1} = \overline{q}/N(q) = 3/10 - j/10$. Môžeme overiť, že naozaj platí vzťah $qq^{-1} = (3 + j)(3/10 - j/10) = 9/10 - j^2/10 = 1$.

[1] V češtine sa namiesto výrazu pole využíva pomenovanie těleso.

1.2 Kvaterniónové algebry

V tejto podkapitole si ukážeme, že štruktúra hamiltonovských kvaterniónov sa dá prirodzeným spôsobom zovšeobecniť do pojmu kvaterniónovej algebry. Okrem samotnej štruktúry zovšeobecníme aj pojmy ako norma, inverzný prvok, atď. Opäť budeme vychádzať z článku Quaternion algebras, K. Conrad [5], ale aj z knihy Quaternion algebras, J. Voight [11].

Poznámka. Odteraz budeme pracovať nad komutatívnym poľom F, pričom predpokladáme, že F nemá charakteristiku 2.

Definícia 1.9 (algebra, dimenzia algebry)**.** *Povieme, že B je* algebra *nad poľom F (resp. F-algebra), ak B je okruh, ktorý je zároveň vektorovým priestorom nad F takým, že násobenie skalárom je kompatibilné s násobením v B v zmysle $(ax)y = x(ay) = a(xy)$ pre všetky $a \in F$, $x, y \in B$.* Dimenziou algebry B *myslíme dimenziu B ako vektorového priestoru nad F.*

Definícia 1.10 (kvaterniónová algebra)**.** *Algebra B nad poľom F je* kvaterniónová algebra*, ak existujú $i, j \in B$ také, že 1, i, j, ij je báza B ako vektorového priestoru nad F a platí $i^2 = a$, $j^2 = b$, $ij = -ji$ pre nejaké $a, b \in F^\times$. Pričom takúto kvaterniónovú algebru budeme značiť $\left(\frac{a,b}{F}\right)$ a prvok ij budeme značiť k.*

Poznámka. Celé násobenie v kvaterniónovej algebre $\left(\frac{a,b}{F}\right)$ je definované pomocou pravidiel z definície 1.9, linearity a asociativity. Pre predstavu môžeme uviesť tabuľku násobenia medzi prvkami i, j a k. Každá bunka tabuľky je súčin označenia riadku s označením stĺpca (v tomto poradí, pričom poradie je dôležité, keďže násobenie nie je komutatívne).

	i	j	k
i	a	k	aj
j	$-k$	b	$-bi$
k	$-aj$	bi	$-ab$

Príklad. Majme kvaterniónovú algebru $\left(\frac{1,2}{\mathbb{R}}\right)$ a v nej prvky $\alpha_1 = i + 2j$, $\alpha_2 = 3 + j + k$. Pozrime sa, ako bude podľa vyššie spomenutých pravidiel v tabuľke vyzerať ich súčin: $\alpha_1\alpha_2 = (i + 2j)(3 + j + k) = 3i + ij + ik + 6j + 2j^2 + 2jk = 3i + k + aj + 6j + 2b - 2bi = 3i + k + j + 6j + 4 - 4i = 4 - i + 7j + k$. V predposlednom kroku výpočtu sme dosadili $a = 1, b = 2$, vzhľadom na to, že pracujeme v kvaterniónovej algebre $\left(\frac{1,2}{\mathbb{R}}\right)$.

Poznámka. Ak si vezmeme kvaterniónovú algebru $\left(\frac{-1,-1}{\mathbb{R}}\right)$, tak ako vektorový priestor ju môžeme vnímať ako $\left(\frac{-1,-1}{\mathbb{R}}\right) = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$. Z definície samotnej algebry navyše vieme, že platí $i^2 = -1$, $j^2 = -1$ a $k = ij = -ji$. Dokopy spolu s linearitou a asociativitou násobenia dostávame, podľa definície 1.1, presne štruktúru kvaterniónov. Ukázali sme, že $\left(\frac{-1,-1}{\mathbb{R}}\right) = \mathbb{H}$. Vďaka čomu vidíme, že kvaterniónová algebra je zovšeobecnením pojmu hamiltonovských kvaterniónov.

Pre kvaterniónové algebry vieme zadefinovať niekoľko ďalších pojmov obdobným spôsobom, ako pre hamiltonovské kvaternióny. Ako sme si už v príklade vyššie mohli všimnúť, pokúsime sa pre lepšiu prehľadnosť dodržať konvenciu, že hamiltonovské kvaternióny budeme značiť obyčajnými malými písmenami a prvky kvaterniónovej algebry malými gréckymi písmenami.

Definícia 1.11 (združený prvok v kvaterniónovej algebre)**.** *Nech prvok* $\alpha \in \left(\frac{a,b}{F}\right)$, $\alpha = t + xi + yj + zk$. *Potom definujeme k nemu* združený prvok $\overline{\alpha}$ *ako* $\overline{\alpha} = t - xi - yj - zk$.

Definícia 1.12 (norma v kvaterniónovej algebre)**.** *Nech* $\alpha = t + xi + yj + zk$, $\alpha \in \left(\frac{a,b}{F}\right)$. *Potom* normu α *definujeme ako* $N(\alpha) = \alpha\overline{\alpha} = t^2 - ax^2 - by^2 + abz^2$.

Definícia 1.13 (stopa v kvaterniónovej algebre)**.** *Nech* $\alpha = t + xi + yj + zk$, $\alpha \in \left(\frac{a,b}{F}\right)$. *Potom* stopu α *definujeme ako* $Tr(\alpha) = \alpha + \overline{\alpha} = 2t$.

Príklad. Opäť predpokladajme, že sme v kvaterniónovej algebre $\left(\frac{1,2}{\mathbb{R}}\right)$ a chceme určiť normu prvku $\alpha = 3+j$. Platí $N(\alpha) = \alpha\overline{\alpha} = (3+j)(3-j) = 9-j^2 = 9-2 = 7$.

Tvrdenie 1.14 (multiplikativita normy a linearita stopy)**.** *Nech* $\alpha_1, \alpha_2 \in \left(\frac{a,b}{F}\right)$. *Potom platí* $N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$ *a* $Tr(\alpha_1 + \alpha_2) = Tr(\alpha_1) + Tr(\alpha_2)$.

Multiplikativita normy sa dá dokázať obdobne ako v tvrdení 1.5. Linearitu stopy je možné ľahko nahliadnuť priamo z definície.

Tvrdenie 1.15 (inverzný prvok v kvaterniónovej algebre)**.** *Nech* $\alpha \in \left(\frac{a,b}{F}\right)$ *a platí, že* $N(\alpha) \neq 0$. *Potom k nemu existuje z oboch strán inverzný prvok a je rovný* $\alpha^{-1} = \overline{\alpha}/N(\alpha)$.

Pre prvky s nenulovou normou vychádzame pri definícii inverzného prvku opäť zo vzťahu $N(\alpha) = \alpha\overline{\alpha}$. Naopak, ak má prvok nulovú normu, tak k nemu neexistuje inverzný prvok. Predpokladajme, že by $N(\alpha) = 0$ a zároveň existovala β taká, že $\alpha\beta = 1$. Potom z multiplikativity normy dostávame $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta) = 0$, čo je spor.

Príklad. Opäť vyrátame inverzný prvok k $\alpha = 3+j$, ale tentokrát v kvaterniónovej algebre $\left(\frac{1,2}{\mathbb{R}}\right)$. Ako už vieme, tak združený prvok je $\overline{\alpha} = 3 - j$ a platí $N(\alpha) = 7$. To znamená, že inverzný prvok bude $\alpha^{-1} = \overline{\alpha}/N(\alpha) = 3/7 - j/7$. Môžeme overiť, že naozaj platí $\alpha\alpha^{-1} = (3+j)(3/7 - j/7) = 9/7 - j^2/7 = 9/7 - 2/7 = 1$.

Pri hamiltonovských kvaterniónoch sme ukázali, že tvoria nekomutatívne pole. Pre kvaterniónovú algebru to vo všeobecnosti neplatí, pretože v nej môžu existovať nenulové prvky, ktoré majú normu rovnú 0, a teda nemajú inverz. Medzi kvaterniónovými algebrami nad $\mathbb{Q}$ ale vieme popísať niektoré z tých, pre ktoré to platí.

Veta 1.16. *Nech* $a \in \mathbb{Z}$, p *je nepárne prvočíslo také, že* $a \not\equiv s^2 \mod p$ *pre* $s \in \mathbb{Z}$. *Potom platí, že* $\left(\frac{a,p}{\mathbb{Q}}\right)$ *je nekomutatívne pole.*

Dôkaz. Ukážeme, že ak vezmeme prvok $\alpha \in \left(\frac{a,p}{\mathbb{Q}}\right)$ taký, že $N(\alpha) = 0$, tak potom nutne $\alpha = 0$. Z toho už priamo plynie, že $\left(\frac{a,p}{\mathbb{Q}}\right)$ je nekomutatívne pole, keďže pre každý nenulový prvok budeme mať inverz. Vezmime si $\alpha = t + xi + yj + zk$ s požadovanými vlastnosťami. Potom z definície normy 1.12 máme:

$$0 = N(\alpha) = N(t+xi+yj+zk) = t^2 - ax^2 - py^2 + apz^2 \Longrightarrow t^2 - ax^2 = p(y^2 - az^2).$$

Môžeme predpokladať, že t, x, y, $z \in \mathbb{Z}$. Ak by to tak nebolo, tak by sme len poslednú rovnosť prenásobili ich spoločným menovateľom. Keďže sme v celých číslach, tak sa na poslednú rovnosť môžeme pozrieť modulo p. Dostaneme:

$$t^2 - ax^2 \equiv 0 \mod p \Longrightarrow t^2 \equiv ax^2 \mod p.$$

Nech $x \not\equiv 0 \mod p$. Potom platí $a \equiv s^2 \mod p$ pre nejaké s, čo je spor s predpokladom. Z toho plynie, že nutne $x \equiv 0 \mod p$. To ale znamená, že $t^2 \equiv 0 \mod p$, a teda $t \equiv 0 \mod p$, keďže p je prvočíslo. Môžeme využiť substitúciu $x = px'$ a $t = pt'$ pre x', $t' \in \mathbb{Z}$. Potom platí:

$$(pt')^2 - a(px')^2 = p(y^2 - az^2) \Longrightarrow p(t'^2 - ax'^2) = y^2 - az^2 \Longrightarrow y^2 \equiv az^2 \mod p.$$

Sme v úplne rovnakej situácii ako pred chvíľou, a obdobne vieme ukázať, že platí $y = py'$, $z = pz'$ pre y', $z' \in \mathbb{Z}$. Po dosadení do našej rovnice získame:

$$p(t'^2 - ax'^2) = (py')^2 - a(pz')^2 \Longrightarrow t'^2 - ax'^2 = p(y'^2 - az'^2).$$

Dopracovali sme sa k rovnakej rovnici ako na začiatku, akurát t, x, y a z sú nahradené za t', x', y' a z'. Môžeme opäť opakovať rovnaký argument a ukázať, že všetky t', x', y', z' sú deliteľné p, atď. V konečnom dôsledku by sme dospeli k tomu, že t, x, y a z sú deliteľné ľubovoľnou mocninou p, a teda musia byť všetky nulové. Ukázali sme, že ak $N(\alpha) = 0$, tak nutne $\alpha = 0$.

□

Príklad. Kvaterniónová algebra $\left(\frac{5,3}{\mathbb{Q}}\right)$ je nekomutatívne pole, pretože $5 \not\equiv s^2 \mod 3$. Dôležité upozornenie ale je, že opačná implikácia z predchádzajúcej vety nutne neplatí.

2. Izomorfizmus kvaterniónových algebier

V tejto kapitole budeme charakterizovať izomorfizmy medzi kvaterniónovými algebrami, pričom väčšina výsledkov pochádza z článku Quaternion algebras, K. Conrad [5]. Izomorfizmom dvoch kvaterniónových algebier nad rovnakým poľom F rozumieme okruhový izomorfizmus $f : B \to B'$, ktorý zároveň fixuje všetky prvky F, teda $\forall a \in F : f(a) = a$.

2.1 Kvaterniónová báza

Definícia 2.1 (kvaterniónová báza)**.** Kvaterniónová báza *je báza kvaterniónovej algebry* $\left(\frac{a,b}{F}\right)$ *tvaru* $\{1, e_1, e_2, e_1e_2\}$*, ak platí, že* $e_1^2 \in F^\times$*,* $e_2^2 \in F^\times$ *a* $e_1e_2 = -e_2e_1$.

Jeden zo spôsobov, ako môžeme skúmať izomorfizmus kvaterniónových algebier, je práve pomocou konštrukcie rôznych kvaterniónových báz. Na začiatok si pomocou toho môžeme dokázať niekoľko základných jednoduchých izomorfizmov.

Lemma 2.2. *Majme kvaterniónovú algebru* $B = \left(\frac{a,b}{F}\right) = F + Fi + Fj + Fk$*. Potom platia nasledujúce izomorfizmy:*

1) $\left(\frac{a,b}{F}\right) \simeq \left(\frac{b,a}{F}\right)$,

2) $\left(\frac{a,b}{F}\right) \simeq \left(\frac{a,-ab}{F}\right)$,

3) $\left(\frac{a,b}{F}\right) \simeq \left(\frac{ac^2,bd^2}{F}\right)$ *pre všetky* $c, d \in F^\times$.

Dôkaz. Nech $\{1, i, j, k\}$ je kvaterniónová báza B, kde $i^2 = a$, $j^2 = b$, $k = ij = -ji$.

1) Rovnako, ako bázu daného vektorového priestoru, môžeme vziať aj $\{1, j, i, k\}$, ktorá je kvaterniónovou bázou, keďže sme len prehodili pozíciu i a j. Odtiaľ:
$$\left(\frac{a,b}{F}\right) \simeq \left(\frac{j^2,i^2}{F}\right) = \left(\frac{b,a}{F}\right).$$

2) Ďalšia možná báza B je $\{1, i, k, aj\}$. Keďže platí $ik = i^2j = aj$, $ki = iji = -ji^2 = -aj$, tak sa jedná o kvaterniónovú bázu, a z toho plynie:
$$\left(\frac{a,b}{F}\right) \simeq \left(\frac{i^2,k^2}{F}\right) = \left(\frac{a,-ab}{F}\right).$$

3) Pre nenulové $c, d \in F$ platí, že aj $\{1, ci, dj, (ci)(dj)\}$ tvorí bázu B. Máme $cidj = cdk$, $djci = -cdk$, čiže sa jedná o kvaterniónovú bázu a odtiaľ:
$$\left(\frac{a,b}{F}\right) \simeq \left(\frac{(ci)^2,(di)^2}{F}\right) = \left(\frac{ac^2,bd^2}{F}\right).$$

Týmto sme dokázali všetky požadované izomorfizmy.

□

Pomocou izomorfizmov z predchádzajúcej vety vieme dosadením konkrétnych hodnôt odvodiť aj niektoré ďalšie, ktoré budeme následne využívať v dôkazoch.Ak do izomorfizmu $\left(\frac{a,b}{F}\right) \simeq \left(\frac{a,-ab}{F}\right)$ dosadíme za $b = 1$, tak dostaneme $\left(\frac{a,1}{F}\right) \simeq \left(\frac{a,-a}{F}\right)$. Využitím $\left(\frac{a,b}{F}\right) \simeq \left(\frac{ac^2,bd^2}{F}\right)$ pre $b = 1, c = 1$ zas dostaneme $\left(\frac{a,1}{F}\right) \simeq \left(\frac{a,d^2}{F}\right)$. Ich spojením potom máme napríklad nový izomorfizmus $\left(\frac{a,-a}{F}\right) \simeq \left(\frac{a,1}{F}\right) \simeq \left(\frac{a,d^2}{F}\right)$.

2.2 Rozštiepiteľné a nerozštiepiteľné kvaternión-ové algebry

V tejto časti bude našim cieľom ukázať, že vo všeobecnosti pre kvaterniónové algebry nad poľom F platí, že až na izomorfizmus sú dvoch typov. Buď bude daná algebra predstavovať nekomutatívne pole, alebo bude izomorfná $M_2(F)$. Následne ešte popíšeme ekvivalentné podmienky, ktoré určujú, ktorý z týchto prípadov nastane. Podľa tohto delenia sa daným typom kvaterniónových algebier hovorí aj rozštiepiteľné alebo nerozštiepiteľné. Pre pripomenutie uveďme, že $M_2(F)$ označuje F-algebru tvorenú maticami typu 2×2 nad poľom F spolu s maticovým sčítavaním a násobením.

Definícia 2.3 (rozštiepiteľná a nerozštiepiteľná kvaterniónová algebra [1])**.** *Kvaterniónová algebra* $\left(\frac{a,b}{F}\right)$ *sa nazýva* rozštiepiteľná kvaterniónová algebra nad F*, ak platí izomorfizmus F-algebier* $\left(\frac{a,b}{F}\right) \simeq M_2(F)$*. Naopak, ak* $\left(\frac{a,b}{F}\right) \not\simeq M_2(F)$*, tak sa* $\left(\frac{a,b}{F}\right)$ *nazýva* nerozštiepiteľná kvaterniónová algebra nad F*.*

Na to, aby sme dokázali, že kvaterniónové algebry sú naozaj daných dvoch typov, ako sme spomínali v úvode, budeme potrebovať nasledujúce dve tvrdenia. Tie priamo popisujú niektoré kvaterniónové algebry, ktoré sú izomorfné $M_2(F)$.

Tvrdenie 2.4. *Pre všetky $a \in F^\times$ platí* $\left(\frac{a,1}{F}\right) \simeq M_2(F)$*.*

Dôkaz. Kvaterniónovú bázu $\{1, i, j, k\}$ kvaterniónovej algebry $\left(\frac{a,1}{F}\right)$ zobrazíme na nasledujúce matice z $M_2(F)$, ktoré sú lineárne nezávislé, a teda tvoria bázu $M_2(F)$:

$$1 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \to \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \quad j \to \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad k \to \begin{pmatrix} 0 & -1 \\ a & 0 \end{pmatrix}.$$

Odtiaľ dané zobrazenie vďaka linearite rozšírime na zobrazenie $\psi : \left(\frac{a,1}{F}\right) \to M_2(F)$ dané vzťahom:

$$t + xi + yj + zk \to \begin{pmatrix} t + y & x - z \\ a(x + z) & t - y \end{pmatrix}.$$

Dané zobrazenie fixuje všetky prvky $a \in F$ v zmysle, že platí $\psi(a) = aI_2$. Zároveň sa dá priamym výpočtom overiť, že pre $\alpha, \beta \in \left(\frac{a,1}{F}\right)$ platia vzťahy $\psi(\alpha + \beta) = \psi(\alpha) + \psi(\beta)$, $\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$ a $\psi(f\alpha) = f\psi(\alpha)$ pre všetky $f \in \mathbb{F}$, a teda sa jedná o homomorfizmus F-algebier.

[1] V angličtine uvádzané pod pojmom split, non-split algebra.

Ďalej ukážeme, že je dané zobrazenie ψ prosté. Predpokladajme, že by existovali $\alpha_1 = t_1 + x_1 i + y_1 i + z_1 \neq \alpha_2 = t_2 + x_2 i + y_2 j + z_2 k$ také, že $\psi(\alpha_1) = \psi(\alpha_2)$. Ak porovnáme v matici jednotlivé prvky, tak dostaneme rovnice:

$$t_1 + y_1 = t_2 + y_2, \qquad t_1 - y_1 = t_2 - y_2, \qquad x_1 - z_1 = x_2 - z_2, \qquad a(x_1 + z_1) = a(x_2 + z_2).$$

Spojením prvých dvoch rovníc vieme odvodiť, že platí $y_2 - y_1 = t_1 - t_2 = y_1 - y_2$, z čoho už priamo plynie $y_1 = y_2$. Odtiaľ potom plynie aj rovnosť $t_1 = t_2$. Keďže $a \in F^\times$, tak ho vieme z poslednej rovnice vykrátiť a máme analogickú situáciu pre x a z, z čoho $x_1 = x_2$ a $z_1 = z_2$. Dokopy sme ukázali, že $\alpha_1 = \alpha_2$, čo je spor s predpokladom, a teda ψ je prosté zobrazenie. Keďže dimenzia $\left(\frac{a,1}{F}\right)$ aj $M_2(F)$ je rovná 4, tak prostý homomorfizmus medzi vektorovými priestormi je izomorfizmus.

□

Príklad. Ukázali sme, že $\left(\frac{a,1}{F}\right) \simeq \left(\frac{a,c^2}{F}\right) \simeq \left(\frac{c^2,a}{F}\right)$ pre $c \in F^\times$. Vďaka poslednému tvrdeniu zas vieme, že všetky tieto kvaterniónové algebry sú izomorfné $M_2(F)$. Na rozštiepiteľnosť teda napríklad stačí, že pre $\left(\frac{a,b}{F}\right)$ je buď a alebo b štvorec v $F^\times$. Pre niektoré kvaterniónové algebry, ako napríklad $\left(\frac{5,9}{\mathbb{R}}\right)$ a $\left(\frac{4,3}{\mathbb{R}}\right)$, tým pádom rovno vidíme, že sú rozštiepiteľné a navzájom izomorfné.

Podmienka, ktorú sme využili v príklade sa dá ešte zoslabiť. Namiesto toho, aby sme požadovali, že b bude štvorec, tak stačí, ak bude v nasledujúcom tvare.

Tvrdenie 2.5. *Ak pre $a, b \in F^\times$ platí, že $b = l^2 - am^2$ pre nejaké $l, m \in F$, potom $\left(\frac{a,b}{F}\right) \simeq M_2(F)$.*

Dôkaz. Majme $b = l^2 - am^2$, kde $l, m \in F$. Vieme, že $\left(\frac{a,b}{F}\right)$ má kvaterniónovú bázu $\{1, i, j, k\}$. Ukážeme, že aj $\{1, i, lj + mk, i(lj + mk)\}$ tvorí inú kvaterniónovú bázu tejto algebry. Vieme, že platí $(lj + mk)^2 = bl^2 - abm^2 = b(l^2 - am^2) = b^2 \in F^\times$. Ak by bola pravda, že $\{1, i, lj + mk, i(lj + mk)\}$ je kvaterniónová báza, tak potom dostaneme:

$$\left(\frac{a,b}{F}\right) \simeq \left(\frac{i^2, (lj + mk)^2}{F}\right) \simeq \left(\frac{a, b^2}{F}\right) \simeq \left(\frac{a,1}{F}\right) \simeq M_2(F).$$

V predposlednom kroku sme využili izomorfizmus, ktorý sme dokázali na konci sekcie 2.1 a v poslednom kroku tvrdenie 2.4.

Najprv overíme, že ak by to bola báza, tak je kvaterniónová. Ako sme už ukázali, tak $i^2 = a \in F^\times$, $(lj + mk)^2 = b^2 \in F^\times$. Na záver ešte máme $i(lj + mk) = lk + amj$, $(lj + mk)i = -lk - amj$, a teda platí, že $i(lj + mk) = -(lj + mk)i$.

Posledným krokom je ukázať, že $\{1, i, lj + mk, i(lj + mk)\}$ je báza $\left(\frac{a,b}{F}\right)$. Všetko sú to prvky danej kvaterniónovej algebry, a teda stačí ukázať, že sú lineárne nezávislé nad F. Potom už vďaka dimenzii určite tvoria jej bázu. Pre posledný prvok platí $i(lj + mk) = amj + lk$. Ak si prvky $\{1, i, lj + mk, amj + lk\}$ zapíšeme do matice vzhľadom k pôvodnej báze $\{1,i,j,k\}$, tak dostaneme:

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & l & am \\ 0 & 0 & m & l \end{pmatrix}.$$

Platí, že dané prvky sú lineárne nezávislé nad F, ak táto matica má lineárne nezávislé stĺpce. To je zas ekvivalentné tomu, že matica je regulárna, čiže jej determinant je nenulový. Pričom môžeme vidieť, že to naozaj platí: $\det A = l^2 - am^2 = b \neq 0$.

□

Príklad. Ak zvolíme $l = m = 1$, tak dostávame, že $b = 1 - a$ je v požadovanom tvare, keďže platí $b = 1 - a = l^2 - am^2$. Z toho priamo podľa posledného tvrdenia 2.5 dostávame nový izomorfizmus tvaru $\left(\frac{a,1-a}{F}\right) \simeq M_2(F)$.

Lemma 2.6. *Nech $a \in F^\times$. Potom množina nenulových prvkov tvaru $l^2 - am^2$ pre $l, m \in F$ je podgrupa $F^\times$.*

Dôkaz. Ak vezmeme $l = 1$ a $m = 0$, tak vidíme, že 1 patrí do tejto množiny. Ďalej overíme uzavretosť na násobenie. Predpokladajme, že $l_1^2 - am_1^2, l_2^2 - am_2^2$ patria do danej množiny. Potom platí, že aj ich súčin je v danej množine:

$$\begin{aligned}(l_1^2 - am_1^2)(l_2^2 - am_2^2) &= l_1^2 l_2^2 + a^2 m_1^2 m_2^2 - a l_1^2 m_2^2 - a l_2^2 m_1^2 \\ &= (l_1 l_2 + a m_1 m_2)^2 - 2a l_1 l_2 m_1 m_2 - a l_1^2 m_2^2 - a l_2^2 m_1^2 \\ &= (l_1 l_2 + a m_1 m_2)^2 - a(l_1 m_2 + l_2 m_1)^2.\end{aligned}$$

A na záver overíme uzavretosť na inverzný prvok. Nech $l^2 - am^2$ patrí do danej množiny, potom vieme ukázať, že aj k nemu inverzný prvok tam patrí:

$$\frac{1}{l^2 - am^2} = \frac{l^2 - am^2}{(l^2 - am^2)^2} = \left(\frac{l}{l^2 - am^2}\right)^2 - a\left(\frac{m}{l^2 - am^2}\right)^2.$$

□

V tejto chvíli už máme všetky potrebné nástroje na to, aby sme ukázali tvrdenie spomínané v úvode, a teda, že kvaterniónové algebry sú naozaj dvoch nasledujúcich typov.

Veta 2.7. *Kvaterniónová algebra $\left(\frac{a,b}{F}\right)$, ktorá nie je nekomutatívnym poľom je izomorfná $M_2(F)$.*

Dôkaz. Vezmime si kvaterniónovú algebru $\left(\frac{a,b}{F}\right)$, ktorá nie je nekomutatívnym poľom. Vychádzajúc z izomorfizmov, ktoré sme dokázali na konci sekcie 2.1 a v tvrdení 2.4 dostávame:

$$\left(\frac{d^2, c}{F}\right) \simeq \left(\frac{c, d^2}{F}\right) \simeq \left(\frac{c, 1}{F}\right) \simeq M_2(F).$$

Môžeme teda rovno predpokladať, že a ani b nie sú štvorce v F, pretože inak už vieme, že tvrdenie platí.

To, že $\left(\frac{a,b}{F}\right)$ nie je nekomutatívnym poľom znamená, že existuje nenulový prvok $\alpha \in \left(\frac{a,b}{F}\right)$, ktorý nemá inverz. Ako sme rovno za definíciou 1.15 ukázali, tak to znamená, že $N(\alpha) = 0$. Nech platí $\alpha = t + xi + yj + zk$, tak potom máme $N(\alpha) = t^2 - ax^2 - by^2 + abz^2 = 0$. Odtiaľ úpravou dostávame $t^2 - ax^2 = b(y^2 - az^2)$.

Predpokladajme, že $y^2 - az^2 = 0$, čiže $y^2 = az^2$. Keďže ale a nie je štvorec v F, tak musí platiť $y = z = 0$. Následne však máme $t^2 - ax^2 = 0$, z čoho rovnakou úvahou dostaneme $t = x = 0$. To by ale znamenalo, že $\alpha = 0$, čo je spor. Musí nutne platiť $y^2 - az^2 \neq 0$. Potom vieme vyjadriť b ako $(t^2 - ax^2)/(y^2 - az^2)$. Podľa lemmy 2.6 je b opäť v tvare nenulového $l^2 - am^2$ pre nejaké $l, m \in F$. Následne vďaka tvrdeniu 2.5 dostávame izomorfizmus $\left(\frac{a,b}{F}\right) \simeq M_2(F)$.

□

Vo vete 2.7 sme ukázali, že každá kvaterniónová algebra je buď rozštiepiteľná, a teda izomorfná $M_2(F)$, alebo je nerozštiepiteľná, a teda tvorí nekomutatívne pole. Teraz už vieme, aké možnosti prichádzajú do úvahy. V nasledujúcich vetách dokážeme ekvivalentné podmienky, ktoré nám hovoria o tom, kedy jednotlivé prípady nastávajú. Pomocou práve zisteného vieme ukázať, že podmienka z tvrdenia 2.5 nie je len postačujúca, ale dokonca nutná. Máme teda nasledujúcu vetu, ktorá rozširuje tvrdenie 2.5 aj o druhú implikáciu.

Veta 2.8. *Nech $a, b \in F^\times$. Nasledujúce tvrdenia sú ekvivalentné:*

1) $\left(\frac{a,b}{F}\right) \simeq M_2(F)$ (resp. daná algebra je rozštiepiteľná),

2) $b = l^2 - am^2$ pre nejaké $l, m \in F$.

Dôkaz. 2) $\Rightarrow$ 1): Túto implikáciu sme už dokázali v tvrdení 2.5.

1) $\Rightarrow$ 2): Nech $\left(\frac{a,b}{F}\right) \simeq M_2(F)$. Chceme ukázať, že existujú $l, m \in F$ také, že $b = l^2 - am^2$. Predpokladajme, že a nie je štvorec. Keďže $\left(\frac{a,b}{F}\right) \simeq M_2(F)$, tak vieme, že $\left(\frac{a,b}{F}\right)$ nie je nekomutatívne pole. S týmito predpokladmi sa ale nachádzame v rovnakej situácií, ako v predchádzajúcom dôkaze vety 2.7 a zopakovaním rovnakého argumentu opäť dostaneme $b = l^2 - am^2$ pre nejaké $l, m \in F$.

Teraz predpokladajme, že a je štvorec v F. Ukážeme, že $F^\times$ je podmnožina všetkých nenulových výrazov $l^2 - am^2$ pre $l, m \in F$. Potom vďaka tomu, že $b \in F^\times$, máme vyjadrenie b v požadovanom tvare. Nech teda existuje $c \in F^\times$ také, že $a = c^2$. Potom platí:

$$l^2 - am^2 = l^2 - c^2m^2 = l^2 - (cm)^2 = (l - cm)(l + cm).$$

Môžeme využiť substitúciu $x = l - cm$ a $y = l + cm$, keďže z x, y sme schopní naspäť určiť l a m ako $l = (x+y)/2$ a $m = (y-x)/(2c)$. To ale znamená, že platí rovnosť množín:

$$\{l^2 - am^2 \neq 0 \mid l, m \in F\} = \{(l-cm)(l+cm) \neq 0 \mid l,m \in F\} = \{xy \mid x, y \in F^\times\}$$

Voľbou $x = 1$ dostávame $\{xy \mid x, y \in F^\times\} \supseteq \{y \mid y \in F^\times\} = F^\times$.

□

Vďaka izomorfizmu $\left(\frac{a,b}{F}\right) \simeq \left(\frac{b,a}{F}\right)$ by v poslednej vete mohla byť v druhom bode uvedená aj podmienka $a = l^2 - bm^2$ pre nejaké l, $m \in F$. Spojením týchto podmienok vieme dostať nasledujúcu inú charakterizáciu, ktorá je vzhľadom k a a b symetrická.

Veta 2.9. *Nech $a, b \in F^\times$. Nasledujúce tvrdenia sú ekvivalentné:*

1) $\left(\frac{a,b}{F}\right) \simeq M_2(F)$ *(resp. daná algebra je rozštiepiteľná),*

2) rovnica $ax^2 + by^2 = z^2$ *má v* F *aj iné riešenie* (x, y, z) *ako triviálne.*

Dôkaz. 1) $\Rightarrow$ 2): Nech $\left(\frac{a,b}{F}\right) \simeq M_2(F)$. Potom podľa vety 2.8 existujú $l, m \in F$ také, že $b = l^2 - am^2$. Keďže $\left(\frac{a,b}{F}\right) \simeq \left(\frac{b,a}{F}\right)$, tak analogicky podľa vety 2.8 existujú aj $n, o \in F$ také, že $a = n^2 - bo^2$. Vieme odvodiť, že platí:

$$am^2 = am^2 \Longrightarrow am^2 = (n^2 - bo^2)m^2 \Longrightarrow am^2 + b(om)^2 = (nm)^2,$$

$$bo^2 = bo^2 \Longrightarrow bo^2 = (l^2 - am^2)o^2 \Longrightarrow a(mo)^2 + bo^2 = (lo)^2.$$

Ak je m alebo o nenulové, tak vidíme, že sme rovno našli netriviálne riešenie (m, om, nm) alebo (mo, o, lo). Predpokladajme, že by platilo $m = o = 0$, potom máme $a = n^2$, $b = l^2$, kde n a l sú už nutne nenulové. V takom prípade ale platí $a(1/n)^2 + b0^2 = n^2(1/n)^2 = 1^2$ a máme netriviálne riešenie $(1/n, 0, 1)$.

2) $\Rightarrow$ 1): Predpokladajme, že rovnica $ax^2 + by^2 = z^2$ má v F netriviálne riešenie (x,y,z). Potom platí, že buď $x \neq 0$ alebo $y \neq 0$, pretože ak by $x = y = 0$, tak rovno aj $z = 0$, čo je spor. Bez ujmy na všeobecnosti predpokladajme, že $y \neq 0$, a teda $y^2 \neq 0$. Potom platí $a(x/y)^2 + b = (z/y)^2$, čo vieme prepísať ako $b = (z/y)^2 - a(x/y)^2$. Následne vďaka vete 2.8 vieme, že $\left(\frac{a,b}{F}\right) \simeq M_2(F)$.

□

Priamo negáciou jednotlivých tvrdení z vety 2.9 dostávame ako dôsledok nasledujúcu charakterizáciu.

Veta 2.10. *Nech $a, b \in F^\times$. Nasledujúce tvrdenia sú ekvivalentné:*

1) $\left(\frac{a,b}{F}\right)$ *je nekomutatívne pole (resp. daná algebra je nerozštiepiteľná),*

2) rovnica $ax^2 + by^2 = z^2$ *má v* F *iba triviálne riešenie* $(x, y, z) = (0,0,0)$.

2.3 Izomorfizmus kvaterniónových algebier nad poľom $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ a $\mathbb{F}_p$

2.3.1 Kvaterniónové algebry nad $\mathbb{R}$

Vo všeobecnosti sme dokázali, že ak nie je kvaterniónová algebra izomorfná $M_2(F)$, tak potom platí, že je nekomutatívnym poľom. Nad reálnymi číslami vieme túto situáciu ešte konkretizovať a dokázať, že dané nekomutatívne pole, ktorému bude algebra izomorfná, budú hamiltonovské kvaternióny. Navyše vieme efektívne charakterizovať, ktorá z týchto dvoch možností nastane. Všetko toto zhrnieme v nasledujúcej vete.

Veta 2.11. *Nech* $\left(\frac{a,b}{\mathbb{R}}\right)$ *je kvaterniónová algebra nad* $\mathbb{R}$. *Potom platí:*

$$\left(\frac{a,b}{\mathbb{R}}\right) \simeq \begin{cases} \mathbb{H} & \text{ak } a < 0 \text{ a zároveň } b < 0, \\ M_2(\mathbb{R}) & \text{ak } a > 0 \text{ alebo } b > 0. \end{cases}$$

Dôkaz. Najprv predpokladajme, že máme $a, b \in \mathbb{R}$ také, že $a < 0$, $b < 0$. Pripomeňme, že pre hamiltonovské kvaternióny platí $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right) = \mathbb{R}+\mathbb{R}i+\mathbb{R}j+\mathbb{R}k$, kde $i^2 = j^2 = -1$, $ij = -ji = k$. To znamená, že $\{1, i, j, k\}$ je kvaterniónová báza $\mathbb{H}$. Potom ukážeme, že aj $\{1, \sqrt{-a}i, \sqrt{-b}j, \sqrt{ab}k\}$ je kvaterniónová báza $\mathbb{H}$. Zjavne je to báza, keďže sme jednotlivé prvky len prenásobili reálnymi číslami. Navyše platí $(\sqrt{-a}i)^2 = -ai^2 = a \in \mathbb{R}$, $(\sqrt{-b}j)^2 = -bj^2 = b \in \mathbb{R}$ a $(\sqrt{-a}i)(\sqrt{-b}j) = \sqrt{ab}k = -\sqrt{ab}(-k) = -(\sqrt{-b}j)(\sqrt{-a}i)$. Z toho, že $\{1, \sqrt{-a}i, \sqrt{-b}j, \sqrt{ab}k\}$ je kvaterniónová báza $\mathbb{H}$ dostávame izomorfizmus:

$$\left(\frac{a, b}{\mathbb{R}}\right) \simeq \left(\frac{(\sqrt{-a}i)^2, (\sqrt{-b}j)^2}{\mathbb{R}}\right) \simeq \mathbb{H}.$$

Teraz bez ujmy na všeobecnosti predpokladajme, že máme $a, b \in \mathbb{R}$ také, že $a < 0$, $b > 0$. Inak by sme využili izomorfizmus $\left(\frac{a,b}{\mathbb{R}}\right) \simeq \left(\frac{b,a}{\mathbb{R}}\right)$. Pozrime sa teraz na kvaterniónovú algebru $\left(\frac{-1,1}{\mathbb{R}}\right) = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$, kde $i^2 = -1$, $j^2 = 1$ a $ij = -ji = k$. Priamo z definície je $\{1, i, j, k\}$ kvaterniónová báza tejto algebry, a tým pádom rovno vieme, že aj $\{1, \sqrt{-a}i, \sqrt{b}j, \sqrt{-ab}k\}$ je báza. Platí, že je to dokonca kvaterniónová báza, keďže $(\sqrt{-a}i)^2 = -ai^2 = a \in \mathbb{R}$, $(\sqrt{b}j)^2 = bj^2 = b \in \mathbb{R}$ a $(\sqrt{-a}i)(\sqrt{b}j) = \sqrt{-ab}k = -\sqrt{-ab}(-k) = -(\sqrt{b}j)(\sqrt{-a}i)$. Vďaka tomu máme izomorfizmus:

$$\left(\frac{a, b}{\mathbb{R}}\right) \simeq \left(\frac{(\sqrt{-a}i)^2, (\sqrt{b}j)^2}{\mathbb{R}}\right) \simeq \left(\frac{-1, 1}{\mathbb{R}}\right) \simeq M_2(\mathbb{R}).$$

Pričom posledná úprava platí vďaka tvrdeniu 2.4.

□

2.3.2 Kvaterniónové algebry nad $\mathbb{C}$

Ukázali sme, že nad reálnymi číslami existujú až na izomorfizmus iba dve kvaterniónové algebry. Nad komplexnými číslami je situácia ešte jednoduchšia. Vieme ukázať, že dokonca všetky kvaterniónové algebry nad $\mathbb{C}$ sú rozštiepiteľné.

Veta 2.12. *Nech* $\left(\frac{a,b}{\mathbb{C}}\right)$ *je kvaterniónová algebra nad* $\mathbb{C}$. *Potom platí* $\left(\frac{a,b}{\mathbb{C}}\right) \simeq M_2(\mathbb{C})$.

Dôkaz. Opäť raz vychádzajúc z izomorfizmov, ktoré sme dokázali na konci sekcie 2.1 a v tvrdení 2.4, dostávame pre všetky $a, c \in \mathbb{C}^\times$ nasledujúci vzťah:

$$\left(\frac{a, c^2}{\mathbb{C}}\right) \simeq \left(\frac{a, 1}{\mathbb{C}}\right) \simeq M_2(\mathbb{C}).$$

V komplexných číslach vieme, že každé číslo je štvorec. Inak povedané, pre všetky $b \in \mathbb{C}^\times$ existuje $c \in \mathbb{C}^\times$ také, že $b = c^2$. A preto pre ľubovoľnú zadanú kvaterniónovú algebru $\left(\frac{a,b}{\mathbb{C}}\right)$ platí:

$$\left(\frac{a, b}{\mathbb{C}}\right) \simeq \left(\frac{a, c^2}{\mathbb{C}}\right) \simeq M_2(\mathbb{C}).$$

Dokázali sme, že každá kvaterniónová algebra nad $\mathbb{C}$ je rozštiepiteľná.

□

2.3.3 Kvaterniónové algebry nad $\mathbb{Q}$

Zatiaľ čo nad $\mathbb{R}$ existujú až na izomorfizmus len dve kvaterniónové algebry a nad $\mathbb{C}$ len jedna, tak nad $\mathbb{Q}$ je situácia oveľa zložitejšia. Dá sa ukázať, že nad racionálnymi číslami existuje nekonečne mnoho neizomorfných kvaterniónových algebier. K dôkazu budeme potrebovať ešte jednu kľúčovú charakterizáciu, ktorú uvedieme vo vete 2.16, ktorá popisuje kedy sú dve kvaterniónové algebry izomorfné.

Lemma 2.13. *Nech* $\left(\frac{a,b}{F}\right) = F + Fi + Fj + Fk$ *je kvaterniónová algebra a* $\alpha \in \left(\frac{a,b}{F}\right)$. *Ak platí* $\alpha i = -i\alpha$, *potom* $\alpha \in Fj + Fk$.

Dôkaz. Nech $\alpha = t + xi + yj + zk$, $\alpha \in \left(\frac{a,b}{F}\right)$ a platí $\alpha i = -i\alpha$. Vyjadríme jednotlivé súčiny:

- $\alpha i = (t + xi + yj + zk)i = ti + ax - yk - azj$,
- $-i\alpha = -i(t + xi + yj + zk) = -ti - ax - yk - azj$.

Potom dostávame:

$$\alpha i = -i\alpha \Longrightarrow ti + ax - yk - azj = -ti - ax - yk - azj \Longrightarrow ti + ax = -ti - ax$$

To znamená, že potrebujeme, aby platilo $t = -t$, $x = -x$. Z čoho dostávame, že $t = 0$, $x = 0$ a α je tvaru $\alpha = yj + zk$. Ukázali sme, že prvok, ktorý antikomutuje s i je nutne z $Fj + Fk$.

□

Predtým, ako dokážeme charakterizáciu vo vete 2.16, tak uvedieme bez dôkazu ešte jednu všeobecnejšiu vetu o konjugovaní koreňov ireducibilného polynómu za určitých podmienok, ktoré ale v našej situácii následne budú splnené. Jedná sa o vetu, na ktorú sa vo svojom článku Quaternion algebras [5] odkazuje aj K. Conrad a jej dôkaz môžeme nájsť v knihe A First Course in Noncommutative Rings, T. Y. Lam [9].

Definícia 2.14 (centrum okruhu)**.** *Množina prvkov okruhu, ktoré komutujú so všetkými prvkami daného okruhu, označujeme* centrum.

Poznámka. Centrom hamiltonovských kvaterniónov sú reálne čísla. Pre kvaterniónovú algebru $\left(\frac{a,b}{F}\right)$ zas platí, že jej centrom je F.

Veta 2.15. *Nech* D *je nekomutatívne pole s centrom* F *a* $f(t)$ *je ireducibilný polynóm v* $F[t]$. *Ak pre* $x, y \in D$ *platí, že* $f(x) = f(y) = 0$, *tak potom existuje* $d \in D^\times$ *také, že* $y = dxd^{-1}$.

Veta 2.16. *Nech* $a, b, c \in F^\times$. *Nasledujúce tvrdenia sú ekvivalentné:*

1) $\left(\frac{a,b}{F}\right) \simeq \left(\frac{a,c}{F}\right)$,

2) $b/c = l^2 - am^2$ *pre nejaké* $l, m \in F$.

Dôkaz. 2) $\Rightarrow$ 1): Majme $b/c = l^2 - am^2$, kde $l,\ m \in F$. Vieme, že $\left(\frac{a,c}{F}\right)$ má kvaterniónovú bázu $\{1, i, j, k\}$. Dokážeme, že aj $\{1, i, lj + mk, i(lj + mk)\}$ je kvaterniónová báza tejto algebry. To, že to je báza, sme dokazovali už v tvrdení 2.5 a tento argument sa dá analogicky použiť. Zároveň vieme, že platí $i^2 = a \in F^\times$, $(lj + mk)^2 = cl^2 - acm^2 = c(l^2 - am^2) = c(b/c) = b \in F^\times$ a aj $i(lj + mk) = lk + amj$, $(lj + mk)i = -lk - amj$. Z toho plynie, že daná báza je kvaterniónová. Spojením týchto tvrdení máme izomorfizmus:

$$\left(\frac{a, c}{F}\right) \simeq \left(\frac{i^2, (lj + mk)^2}{F}\right) \simeq \left(\frac{a, b}{F}\right).$$

1) $\Rightarrow$ 2): Nech platí $\left(\frac{a,b}{F}\right) \simeq \left(\frac{a,c}{F}\right)$. Následne dôkaz tejto implikácie rozdelíme na dve časti. Najprv predpokladajme, že $\left(\frac{a,b}{F}\right) \simeq \left(\frac{a,c}{F}\right) \simeq M_2(F)$. Potom podľa vety 2.8 existujú $l_1,\ m_1,\ l_2,\ m_2 \in F$ také, že $b = l_1^2 - am_1^2$, $c = l_2^2 - am_2^2$. Podľa lemmy 2.6 takéto nenulové prvky tvoria grupu, a teda aj pre b/c existujú $l, m \in F$ také, že $b/c = l^2 - am^2$.

Teraz predpokladajme, že $\left(\frac{a,b}{F}\right), \left(\frac{a,c}{F}\right)$ nie sú izomorfné $M_2(F)$, čiže sú to nekomutatívne polia. V tom prípade podľa príkladu za tvrdením 2.4 a, b ani c nie sú štvorce v F. Opäť predpokladajme, že $\{1, i, j, k\}$ je kvaterniónová báza $\left(\frac{a,c}{F}\right)$, a teda platí $i^2 = a$, $j^2 = c$, $ij = -ji = k$. Keďže $\left(\frac{a,b}{F}\right) \simeq \left(\frac{a,c}{F}\right)$, tak musí pre $\left(\frac{a,c}{F}\right)$ existovať aj kvaterniónová báza $\{1, i', j', k'\}$ taká, že platí $i'^2 = a$, $j'^2 = b$, $i'j' = -j'i' = k'$.

Keďže a nie je v F štvorec, tak potom polynóm $f(x) = x^2 - a$ je ireducibilný nad F. Zároveň v $\left(\frac{a,c}{F}\right)$ platí, že $f(i) = i^2 - a = 0$ aj $f(i') = i'^2 - a = 0$. Využitím vety 2.15 dostávame, že existuje prvok $\alpha \in \left(\frac{a,c}{F}\right)$, $\alpha \neq 0$ taký, že platí $i = \alpha i' \alpha^{-1}$. Následne označme $\beta = \alpha j' \alpha^{-1}$. Potom platia vzťahy:

$$\beta^2 = (\alpha j' \alpha^{-1})(\alpha j' \alpha^{-1}) = \alpha j' j' \alpha^{-1} = \alpha b \alpha^{-1} = b,$$

$$i'j' = -j'i' \Longrightarrow (\alpha i' \alpha^{-1})(\alpha j' \alpha^{-1}) = -(\alpha j' \alpha^{-1})(\alpha i' \alpha^{-1}) \Longrightarrow i\beta = -\beta i.$$

Podľa lemmy 2.13 prvky, ktoré antikomutujú s i sú práve prvky z $Fj + Fk$. To znamená, že existujú $l, m \in F$ také, že $\beta = lj + mk$. Spojením týchto úvah máme:

$$b = \beta^2 = (lj + mk)^2 = l^2 j^2 + lmjk + lmkj + m^2 k^2 = l^2 j^2 + m^2 k^2 = cl^2 - acm^2$$

Odtiaľ dostávame, že $b/c = l^2 - am^2$ pre nejake $l, m \in F$.

□

Môžeme si ešte všimnúť, že veta 2.8 obsahuje podobnú charakterizáciu a je vlastne len konkrétnym prípadom vety 2.16 ak za c dosadíme 1. Táto jednoduchšia verzia sa však priamo využívala v dôkaze. Teraz už máme všetko potrebné na to, aby sme sa vrátili k dôkazu existencie nekonečne mnoho neizomorfných kvaterniónových algebier nad $\mathbb{Q}$.

Dôsledok 2.17. *Nech p, q sú rôzne prvočísla také, že $p \equiv 3 \mod 4$, $q \equiv 3 \mod 4$. Potom platí $\left(\frac{-1,p}{\mathbb{Q}}\right) \not\simeq \left(\frac{-1,q}{\mathbb{Q}}\right)$. Z toho plynie, že existuje nekonečne mnoho neizomorfných kvaterniónových algebier nad $\mathbb{Q}$.*

Dôkaz. Daný dôkaz bude konštruktívny. Ukážeme, že pre rôzne prvočísla p, q také, že $p \equiv 3 \mod 4$, $q \equiv 3 \mod 4$, platí $\left(\frac{-1,p}{\mathbb{Q}}\right) \not\simeq \left(\frac{-1,q}{\mathbb{Q}}\right)$. Keďže existuje nekonečne veľa prvočísel kongruentných 3 modulo 4, tak sme týmto skonštruovali nekonečne mnoho neizomorfných kvaterniónových algebier nad $\mathbb{Q}$.

Nech p, q prvočísla, $p \neq q$, $p \equiv 3 \mod 4$ a $q \equiv 3 \mod 4$. Budeme postupovať sporom. Predpokladajme, že $\left(\frac{-1,p}{\mathbb{Q}}\right) \simeq \left(\frac{-1,q}{\mathbb{Q}}\right)$. Podľa vety 2.16 potom platí, že existujú $l, m \in \mathbb{Q}$ také, že $q/p = l^2 + m^2$. Nájdime $a, b, d \in \mathbb{Z}$, $d \neq 0$ také, že platí $l = a/d$ a $m = b/d$. Potom danú rovnicu vieme prepísať nasledovne:

$$q/p = l^2 + m^2 \Longrightarrow q/p = (a/d)^2 + (b/d)^2 \Longrightarrow d^2q = p(a^2 + b^2).$$

Ľavá strana rovnice je deliteľná q, takže aj pravá musí byť. Keďže p je prvočíslo rôzne od q, tak nutne platí, že a^2+b^2 je deliteľné q. Odtiaľ ukážeme, že obe a aj b sú deliteľné q. Ak by jedno z nich bolo deliteľné q, tak už nutne bude aj druhé z nich. Preto predpokladajme, že a ani b nie sú deliteľné q, čiže $NSD(a, q) = NSD(b,q) = 1$. Potom vieme nasledujúcim spôsobom ukázať, že -1 je kvadratický zvyšok modulo q:

$$a^2 + b^2 \equiv 0 \mod q \Longrightarrow a^2 \equiv -b^2 \mod q \Longrightarrow (a/b)^2 \equiv -1 \mod q.$$

Keď sa na to pozrieme ale z definície cez Legendrov symbol $\left(\frac{-1}{q}\right)$, tak dostávame $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}} = -1$, keďže $q \equiv 3 \mod 4$. To ale znamená, že -1 je kvadratický nezvyšok modulo q, čo je spor. Tým pádom a aj b sú deliteľné q, a teda $a^2 + b^2$ je deliteľné q^2.

Vrátime sa k rovnici $d^2q = p(a^2 + b^2)$. Teraz už vieme, že pravá strana je deliteľná q^2, a teda aj výraz na ľavej strane d^2q je deliteľný q^2. Z toho plynie, že d^2, a teda rovno aj d je deliteľné q. Zistili sme, že existujú a', b', $d' \in \mathbb{Z}$ také, že platí $a/q = a'$, $b/q = b'$, $d/q = d'$. Potom:

$$d^2q = p(a^2 + b^2) \Longrightarrow (d'q)^2q = p((a'q)^2 + (b'q)^2) \Longrightarrow (d')^2q = p((a')^2 + (b')^2).$$

Dopracovali sme sa k rovnakej rovnici a úplne analogicky by sme teraz mohli ukázať, že a', b', d' sú všetky deliteľné q. To by znamenalo, že d je deliteľné ľubovoľne vysokou mocninou prvočísla q, čo je spor.

□

2.3.4 Kvaterniónové algebry nad $\mathbb{F}_p$

Nad konečnými telesami $\mathbb{F}_p$ pre nepárne p je situácia podobná ako nad $\mathbb{C}$. Vieme tiež ukázať, že všetky kvaterniónové algebry nad $\mathbb{F}_p$ sú rozštiepiteľné, a teda izomorfné $M_2(\mathbb{F}_p)$.

Veta 2.18. *Nech p je nepárne prvočíslo a $\left(\frac{a,b}{\mathbb{F}_p}\right)$ je kvaterniónová algebra nad $\mathbb{F}_p$. Potom platí $\left(\frac{a,b}{\mathbb{F}_p}\right) \simeq M_2(\mathbb{F}_p)$.*

Dôkaz. Vezmime kvaterniónovú algebru $\left(\frac{a,b}{\mathbb{F}_p}\right)$. Podľa tvrdenia 2.5 stačí, ak ukážeme, že $b = l^2 - am^2$ pre nejaké l, $m \in \mathbb{F}_p$. Potom už nutne bude platiť izomorfizmus $\left(\frac{a,b}{\mathbb{F}_p}\right) \simeq M_2(\mathbb{F}_p)$.

Chceme teda ukázať, že v $\mathbb{F}_p$ existuje riešenie (l, m) rovnice $b = l^2 - am^2$. Prepíšeme ju do tvaru $b+am^2 = l^2$. Keďže sme v $\mathbb{F}_p$, tak môžeme zrátať počet rôznych hodnôt, ktoré každá strana rovnice môže nadobudnúť. V $\mathbb{F}_p$ máme $(p+1)/2$ štvorcov, čo znamená, že pravá strana rovnice l^2 môže nadobúdať $(p + 1)/2$ rôznych hodnôt. Keďže nenulové a, b sú presne dané, tak aj ľavá strana $b + am^2$ môže nadobúdať $(p+1)/2$ rôznych hodnôt. Keďže $(p+1)/2+(p+1)/2 = p+1 > p$, tak dané množiny v $\mathbb{F}_p$ nemôžu byť disjunktné. To znamená, že existuje l, $m \in \mathbb{F}_p$ také, že $b + am^2 = l^2$.

□

3. Lipschitzov a Hurwitzov rád

Predtým, ako sa dostaneme k druhej dôležitej časti tejto práce, a to charakterizácii konečných grúp jednotiek v rádoch v hamiltonovských kvaterniónoch, tak si najprv urobíme krátku odbočku a vysvetlíme, čo vlastne rády v algebrách sú. Následne sa bližšie pozrieme ešte na tri konkrétne príklady, okrem iného aj na Lipschitzov a Hurwitzov rád. Okrem toho, že tieto rády sú sami osebe peknými príkladmi rádov v kvaterniónových algebrách, tak na nich v piatej kapitole pri klasifikácii grúp jednotiek opäť narazíme a jednotlivé dokázané vlastnosti využijeme.

3.1 Rády

V tejto časti budeme ďalej R označovať obor integrity, F jeho podielové pole a B bude značiť konečno-dimenzionálnu F-algebru. Postupovať budeme podľa knihy Quaternion algebras, J.Voight [11, Kapitola 10].

Definícia 3.1 (mriežka)**.** *Nech V je konečno-dimenzionálny vektorový priestor nad F. Potom R-mriežka vo V je konečne generovaný R-podmodul $M \subseteq V$ taký, že $MF = V$.*

Príklad. Vo vektorovom priestore $\mathbb{Q}^n$ nad $\mathbb{Q}$ je $\mathbb{Z}$-mriežka $\mathbb{Z}^n$ a môžeme ju písať v tvare $\mathbb{Z}^n = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_n$. Pre $\mathbb{Q}[i]$ je $\mathbb{Z}$-mriežka $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$.

Definícia 3.2 (rád)**.** *Nech $\mathcal{O} \subseteq B$ je R-mriežka, ktorá je zároveň podokruhom B. Potom hovoríme, že $\mathcal{O}$ je R-*rád*.*

Keďže ďalej budeme pracovať predovšetkým nad $\mathbb{Z}$, tak na $\mathbb{Z}$-mriežku budeme ďalej referovať len ako na mriežku a na $\mathbb{Z}$-rád len ako na rád.

Príklad. Pre nejaké nenulové $a, b \in \mathbb{Z}$ vezmime kvaterniónovú algebru $B = \left(\frac{a,b}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$. Potom mriežka $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k \subseteq B$, ktorá je uzavretá na násobenie, definuje rád.

Definícia 3.3 (maximálny rád)**.** *Nech $\mathcal{O} \subseteq B$ je R-rád. Potom $\mathcal{O}$ je* maximálny rád*, ak nie je vlastne obsiahnutý v inom ráde.*

Teraz sa pozrieme na celistvé prvky v rádoch a zhrnieme si ešte niekoľko tvrdení ohľadom celistvosti, ktoré budeme v ďalšej časti práce potrebovať. Jednotlivé dôkazy je možné nájsť v knihe Quaternion algebras [11, Kapitola 10].

Definícia 3.4 (celistvý prvok)**.** *Nech $\alpha \in B$. Potom hovoríme, že prvok α je celistvý nad R, ak je koreňom nejakého monického polynómu s koeficientami v R.*

Definícia 3.5 (celistvo uzavretý obor integrity)**.** *Povieme, že obor integrity R je* celistvo uzavretý *v F, ak platí, že vždy, ak je prvok $\alpha \in F$ celistvý nad R, tak $\alpha \in R$.*

Príklad. Pre $\mathbb{Q}$ platí, že jediné prvky z $\mathbb{Q}$, ktoré sú celistvé nad $\mathbb{Z}$, sú práve prvky patriace $\mathbb{Z}$. Inými slovami, obor celých čísel $\mathbb{Z}$ je celistvo uzavretý v $\mathbb{Q}$.

Lemma 3.6. *Nech $\alpha \in B$. Potom nasledujúce tvrdenia sú ekvivalentné:*

1) α je celistvá nad R,

2) $R[\alpha]$ je konečne generovaný R-modul,

3) α je obsiahnutá v podokruhu A, ktorý je konečne generovaný ako R-modul.

Vzhľadom na definíciu rádu z predchádzajúcej, pomerne známej lemmy 3.6, plynie priamo nasledujúce tvrdenie.

Tvrdenie 3.7 (celistvé prvky v ráde)**.** *Nech $\mathcal{O}$ je R-rád a $\alpha \in \mathcal{O}$. Potom α je celistvý prvok nad R.*

Ďalšie tvrdenie uvedieme rovno iba pre kvaterniónové algebry, keďže pre tie máme zavedené pojmy normy a stopy.

Tvrdenie 3.8. *Nech B je kvaterniónová algebra nad poľom F a R je celistvo uzavretý obor integrity. Potom $\alpha \in B$ je celistvý prvok nad R práve vtedy, keď $N(\alpha), Tr(\alpha) \in R$.*

Poznámka. V prípade, že budeme mať R-rád $\mathcal{O} \subseteq B$ a bude platiť, že R je celistvo uzavretý obor integrity, tak potom pre všetky prvky rádu $\mathcal{O}$ platí, že ich norma a stopa budú patriť do R. Túto úvahu dostávame spojením tvrdení 3.7 a 3.8 a budeme ju často využívať.

3.2 Lipschitzov rád

V predchádzajúcej podkapitole sme si zadefinovali rády vo všeobecnosti. Teraz prejdeme ku konkrétnym príkladom rádov v kvaterniónových algebrách. Opäť budeme vychádzať z knihy Quaternion algebras [11, Kapitola 11], ktorú doplníme o viaceré vlastné podrobné dôkazy, ktoré sa v knihe nenachádzajú.

Konkrétne sa najprv pozrieme na kvaterniónovú algebru $B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, ktorú môžeme vnímať aj ako $\mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$, pričom $i^2 = j^2 = -1$ a $k = ij = -ji$. Vidíme teda, že kvaterniónová algebra B predstavuje v istom zmysle vlastne zúženie hamiltonovských kvaterniónov s koeficientami v $\mathbb{R}$ na koeficienty v $\mathbb{Q}$. V prípade, že by sme koeficienty zúžili dokonca na $\mathbb{Z}$, tak prirodzene získame nasledujúci rád v tejto algebre.

Definícia 3.9 (Lipschitzov rád)**.** *Rád $\mathbb{Z}\langle i, j\rangle = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ v kvaterniónovej algebre $\left(\frac{-1,-1}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ nazývame* Lipschitzov rád.

Môžeme si všimnúť, že mriežka $\mathbb{Z}\langle i, j\rangle$ je skutočne uzavretá na násobenie, a teda sa podľa definície 3.2 jedná o rád.

Keďže Lipschitzov rád predstavuje isté zúženie hamiltonovských kvaterniónov, tak prvky tohto rádu sa označujú aj ako Lipschitzovské kvaternióny. Teraz sa ešte pozrieme na grupu jednotiek v tomto ráde a ukážeme, že je ňou grupa, ktorú označujeme ako kvaterniónová grupa.

Definícia 3.10 (kvaterniónová grupa)**.** Kvaterniónovou grupou *označujeme nekomutatívnu grupu kvaterniónov $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ rádu 8.*

Tvrdenie 3.11 (jednotky v Lipschitzovom ráde). *Prvok $\alpha \in \mathbb{Z}\langle i,j\rangle$ je jednotkou práve vtedy, keď $N(\alpha) = 1$.*

Dôkaz. Pre každý prvok $\alpha \in \mathbb{Z}\langle i,j\rangle$, $\alpha = t+xi+yj+zk$, podľa definície normy 1.12 platí, že $N(\alpha) = t^2 + x^2 + y^2 + z^2$, keďže v našej kvaterniónovej algebre máme $a = b = -1$. Navyše vďaka tomu, že t, x, y, $z \in \mathbb{Z}$, máme $N(\alpha) \in \mathbb{Z}_0^+$.

Pre prvú implikáciu predpokladajme, že $\alpha \in \mathbb{Z}\langle i,j\rangle^\times$. To z definície znamená, že existuje $\beta \in \mathbb{Z}\langle i,j\rangle$ taká, že platí $\alpha\beta = 1$. Odtiaľ po aplikovaní multiplikativity normy z tvrdenia 1.14 dostávame, že $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$. To v spojení s $N(\alpha), N(\beta) \in \mathbb{Z}_0^+$ znamená, že $N(\alpha) = 1$.

Pre opačnú implikáciu predpokladajme, že $N(\alpha) = 1$. Máme teda rovnosť $1 = N(\alpha) = t^2 + x^2 + y^2 + z^2$, pričom t, x, y, $z \in \mathbb{Z}$. Jediné riešenia, ktoré dostávame, vedú na štvorice (t,x,y,z), kde sú tri prvky rovné 0 a posledný je ± 1. To vedie na kvaternióny $\pm 1, \pm i, \pm j, \pm k$. Posledným krokom je overiť, že každý z týchto ôsmich prvkov je naozaj jednotka. Prvky 1 a -1 sú si samé svojím inverzom. Pre zvyšné prvky tiež platí, že poznáme ich inverz, pretože vzhľadom na to, že sme v kvaterniónovej algebre $\left(\frac{-1,-1}{\mathbb{Q}}\right)$, tak prvky i a $-i$, j a $-j$, k a $-k$ sú si takto po dvojiciach navzájom inverzné.

□

Dôsledok 3.12 (grupa jednotiek Lipschitzovho rádu). *Grupa jednotiek Lipschitzovho rádu je kvaterniónová grupa, teda inak povedané $\mathbb{Z}\langle i,j\rangle^\times = Q_8$.*

Dôkaz. Tvrdenie 3.11 hovorí, že jednotkami sú práve tie prvky, ktoré majú normu rovnú 1. Následne priamo v dôkaze tohto tvrdenia sme ukázali, že v $\mathbb{Z}\langle i,j\rangle$ sa s touto vlastnosťou jedná len o prvky $\pm 1, \pm i, \pm j, \pm k$, a teda $\mathbb{Z}\langle i,j\rangle^\times = Q_8$.

□

3.3 Hurwitzov rád

Nasledujúci rád, ktorý si spomenieme, bude tiež rád v kvaterniónovej algebre $B = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$. Na rozdiel od Lipschitzovho rádu ale povolíme za určitých podmienok aj koeficienty z $\frac{1}{2}\mathbb{Z}$. Pre jednoduchšiu definíciu zavedieme značenie $\omega = \frac{-1+i+j+k}{2}$.

Definícia 3.13 (Hurwitzov rád). *Rád $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\omega$ v kvaterniónovej algebre $\left(\frac{-1,-1}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ nazývame* Hurwitzov rád.

Prvky Hurwitzovho rádu označujeme ako Hurwitzove kvaternióny. Na overenie toho, či je definícia Hurwitzovho rádu korektná, potrebujeme ukázať, že mriežka $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\omega$ je uzavretá na násobenie, a teda sa naozaj jedná o rád v zmysle definície 3.2. Jediné teoreticky problematické členy, ktoré môžu vzniknúť pri násobení dvoch prvkov z $\mathcal{O}$ odpovedajú $k, i\omega, j\omega, \omega i, \omega j$ a ω^2. Ak ukážeme, že tieto prvky patria $\mathcal{O}$, tak je to rád. Pre k platí $k = 1 - i - j + 2\omega$ a napríklad pre $i\omega$ dostávame $i\omega = i(-1+i+j+k)/2 = (-1-i-j+k)/2 = -i-j+(-1+i+j+k)/2 = -i-j+\omega$. Analogickým spôsobom vieme ukázať, že v $\mathcal{O}$ ležia aj prvky $j\omega = (-1+i-j-k)/2$, $\omega i = (-1-i+j-k)/2$, $\omega j = (-1-i-j+k)/2$ a aj $\omega^2 = (-1-i-j-k)/2$.

Je dôležité si uvedomiť, že na prvky Hurwitzovho rádu môžeme pozerať dvoma spôsobmi. Prvok $\alpha \in \mathcal{O}$ môžeme podľa definície zapísať priamo v tvare $\alpha = s + li + mj + n\omega$, kde budú s, l, m, $n \in \mathbb{Z}$. Druhá možnosť je uvedomiť si, čo značenie ω znamená a rozpísať si ho. Potom môžeme α vnímať ako $\alpha = t + xi + yj + zk$, kde však t, x, y, $z \in \frac{1}{2}\mathbb{Z}$. Dôležité je však pozorovanie, že v prípade, ak by pri prvom zápise koeficient n pri ω bol párne číslo, tak sa zbavíme $1/2$ a pre všetky koeficienty v druhom zápise by platilo t, x, y, $z \in \mathbb{Z}$. Naopak, ak by bolo n nepárne, tak potom všetky t, x, y, $z \in \frac{1}{2} + \mathbb{Z}$. Dôležitá je aj opačná implikácia. Platí totiž, že ak $\alpha = t+xi+yj+zk$ a všetky t, x, y, $z \in \mathbb{Z}$ alebo t, x, y, $z \in \frac{1}{2}+\mathbb{Z}$, tak ľahko ukážeme, že potom daný prvok je z Hurwitzovho rádu. Je tomu tak preto, lebo platí: $\alpha = t+xi+yj+zk = (t+z)+(x-z)i+(y-z)j+(2z)\frac{-1+i+j+k}{2}$. Odtiaľ priamo vidíme, že pri daných podmienkach sú všetky koeficienty $t+z$, $x-z$, $y-z$ a $2z$ celé čísla. Toto pozorovanie zhrnieme v nasledujúcej lemme.

Lemma 3.14. *Nech $\alpha \in \left(\frac{-1,-1}{\mathbb{Q}}\right)$, $\alpha = t + xi + yj + zk$. Potom platí, že α patrí do Hurwitzovho rádu práve vtedy, ak všetky t, x, y, $z \in \mathbb{Z}$ alebo t, x, y, $z \in \frac{1}{2}+\mathbb{Z}$.*

Teraz si rovnako, ako pri Lipschitzovom ráde dokážeme, ako vyzerá grupa jednotiek Hurwitzovho rádu a následne aj aký je vzťah medzi týmito dvoma spomínanými rádmi.

Tvrdenie 3.15 (grupa jednotiek Hurwitzovho rádu)**.** *Grupa jednotiek Hurwitzhovho rádu je $\mathcal{O}^\times = \{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}$, čiže grupa rádu 24.*

Dôkaz. Predpokladajme, že $\alpha \in \mathcal{O}^\times$. To znamená, že existuje $\beta \in \mathcal{O}$ taká, že platí $\alpha\beta = 1$. Nech $\alpha = t+xi+yj+zk$ a $\beta = s+li+mj+nk$, kde t, x, y, z, s, l, m, $n \in \frac{1}{2}\mathbb{Z}$. Označme ešte $t_1 = 2t$, čiže $t_1 \in \mathbb{Z}$ a analogicky aj pre všetky ostatné prvky x, y, z, s, l , m, n.

Po aplikovaní normy a jej multiplikativity na rovnosť $\alpha\beta = 1$ dostávame $N(\alpha)N(\beta) = 1$. Z čoho po vyjadrení jednotlivých noriem získame rovnosť $1 = (t^2+x^2+y^2+z^2)(s^2+l^2+m^2+n^2) = (t^2+x^2+y^2+z^2)(s_1^2+l_1^2+m_1^2+n_1^2)/4$. Podľa lemmy 3.14 vieme, že môžu nastať nasledujúce dva prípady.

Buď platí, že t, x, y, $z \in \mathbb{Z}$. Potom nám ale v rovnosti, ktorú sme získali $4 = (t^2+x^2+y^2+z^2)(s_1^2+l_1^2+m_1^2+n_1^2)$ v pozícií neznámych vystupujú iba celé čísla. Zároveň vieme, že každá zo zátvoriek predstavuje nezáporné číslo, a teda v takom prípade máme tri možnosti, ako rozložiť 4 na požadovaný súčin:

- Platí $t^2+x^2+y^2+z^2 = 1$, $s_1^2+l_1^2+m_1^2+n_1^2 = 4$. To znamená, že vlastne $\alpha \in \mathbb{Z}\langle i, j\rangle$ a zároveň $N(\alpha) = 1$. Podľa tvrdenia 3.11 je takáto α jednotkou v Lipschitzovom ráde, a teda $\alpha \in Q_8$ podľa 3.12. Rovno vidíme, že podľa rovnakého argumentu ako v Lipschitzovom ráde sú všetky tieto prvky jednotkami aj v Hurwitzovom ráde.

- Platí $t^2+x^2+y^2+z^2 = 2$, $s_1^2+l_1^2+m_1^2+n_1^2 = 2$. Potom dve z neznámych s_1, l_1, m_1, n_1 sú rovné 1 alebo -1 a zvyšné dve sú rovné 0. Z toho spätne dve z neznámych s, l, n, m sú rovné $\pm 1/2$ a dve 0. To je však podľa lemmy 3.14 spor s tým, že $\beta \in \mathcal{O}$.

- Platí $t^2+x^2+y^2+z^2=4$, $s_1^2+l_1^2+m_1^2+n_1^2=1$. Rovnakou úvahou ako vyššie vieme odvodiť, že práve jedna z neznámych s, l, m, n je rovná $\pm 1/2$ a zvyšné sú nulové. Dostávame rovnaký spor a táto možnosť nevedie na žiadne jednotky v Hurwitzovom ráde.

Alebo potom platí, že t, x, y, $z \in \frac{1}{2}+\mathbb{Z}$. Pôvodnú rovnosť si ešte trochu využitím vzťahov $t_1 = 2t$ atď. upravíme na $16 = (t_1^2+x_1^2+y_1^2+z_1^2)(s_1^2+l_1^2+m_1^2+n_1^2)$, kde opäť platí, že všetky neznáme sú celé čísla. Rozoberieme všetky možnosti, ako rozložiť 16 na súčin:

- Platí $t_1^2+x_1^2+y_1^2+z_1^2=1$, $s_1^2+l_1^2+m_1^2+n_1^2=16$. Potom sú tri z neznámych t_1, x_1, y_1, z_1 nulové, a teda aj tri z t, x, y, z, čo znamená spor s predpokladom t, x, y, $z \in \frac{1}{2}+\mathbb{Z}$.

- Platí $t_1^2+x_1^2+y_1^2+z_1^2=2$, $s_1^2+l_1^2+m_1^2+n_1^2=8$. Úplne ekvivalentne, ako v prvom prípade, akurát budú nulové dve premenné. Čo stále vedie k sporu.

- Platí $t_1^2+x_1^2+y_1^2+z_1^2=4$, $s_1^2+l_1^2+m_1^2+n_1^2=4$. Žiadna z premenných t_1, x_1, y_1, z_1 nemôže byť rovná 2, pretože potom by neplatilo, že t, x, y, $z \in \frac{1}{2}+\mathbb{Z}$. Preto jediná možnosť je $t_1 = x_1 = y_1 = z_1 = \pm 1$. To vedie k tomu, že α je jedným z 16 Hurwitzových kvaterniónov tvaru $(\pm 1 \pm i \pm j \pm k)/2$. Posledným krokom je overiť, že každý z týchto prvkov je jednotkou. To platí, pretože vieme, že každý z týchto 16 prvkov má normu 1, a teda $1 = N(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha$. Zároveň pre každý z týchto 16 prvkov platí, že aj k nemu združený je medzi nimi. A teda sú si po dvojiciach navzájom inverznými prvkami.

- Platí $t_1^2+x_1^2+y_1^2+z_1^2=8$, $s_1^2+l_1^2+m_1^2+n_1^2=2$. Teraz bude najjednoduchšie sa pozrieť na to, že medzi s_1, l_1, m_1, n_1 sú dve neznáme rovné ± 1 a dve rovné 0. Čo je opäť spor s tým, že niektoré z s, l, m, n patria $\mathbb{Z}$ a iné $\frac{1}{2}+\mathbb{Z}$.

- Platí $t_1^2+x_1^2+y_1^2+z_1^2=16$, $s_1^2+l_1^2+m_1^2+n_1^2=1$. Rovnako ako v predchádzajúcom prípade, akurát je nenulová len jedna z nich.

Pri rozbore len dva prípady viedli k nájdeniu jednotiek v Hurwitzovom ráde. Dokopy sme dokázali, že $\mathcal{O}^\times = \{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}$.

□

Tvrdenie 3.16 (vzťah Lipschitzovho a Hurwitzovho rádu)**.** *Hurwitzov rád $\mathcal{O}$ je jediný rád, ktorý vlastne obsahuje Lipschitzov rád $\mathbb{Z}\langle i, j\rangle$.*

Dôkaz. To, že Hurwitzov rád obsahuje vlastne Lipschitzov rád vidíme priamo z definície. Ďalej predpokladajme, že existuje nejaký rád $\mathcal{O}'$ v kvaterniónovej algebre $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ taký, že platí $\mathbb{Z}\langle i, j\rangle \subsetneq \mathcal{O}'$. Nech $\alpha \in \mathcal{O}'$, $\alpha = t + xi + yj + zk$, pričom t, x, y, $z \in \mathbb{Q}$.

Keďže $\mathcal{O}'$ je rád, tak podľa tvrdení 3.7 a 3.8 platí, že $Tr(\alpha) \in \mathbb{Z}$. Odtiaľ dostávame, že $Tr(\alpha) = 2t \in \mathbb{Z}$, čiže $t \in \frac{1}{2}\mathbb{Z}$. Keďže $\alpha \in \mathcal{O}'$, tak potom aj prvky αi, αj, $\alpha k \in \mathcal{O}'$. Po vyčíslení máme $Tr(\alpha i) = Tr(-x + ti + zj - yk) = -2x$, $Tr(\alpha j) = Tr(-y - zi + tj + xk) = -2y$, $Tr(\alpha k) = Tr(-z + yi - xj + tk) = -2z$. Pričom obdobne dostávame, že všetky tieto stopy musia byť celé čísla, a teda $-2x$, $-2y$, $-2z \in \mathbb{Z}$. Odtiaľ x, y, $z \in \frac{1}{2}\mathbb{Z}$.

Zatiaľ sme ukázali, že pre ľubovoľné $\alpha \in \mathcal{O}'$, $\alpha = t + xi + yj + zk$ platí, že t, x, y, $z \in \frac{1}{2}\mathbb{Z}$. Ak ukážeme, že buď t, x, y, $z \in \mathbb{Z}$ alebo t, x, y, $z \in \frac{1}{2} + \mathbb{Z}$, tak potom je $\mathcal{O}'$ nutne Hurwitzov rád. Označme $t_1 = 2t$, čiže nutne $t_1 \in \mathbb{Z}$ a analogicky aj pre zvyšné prvky x, y, z. Podľa tvrdení 3.7 a 3.8 platí, že $N(\alpha) \in \mathbb{Z}$. Z definície normy dostávame, že $N(\alpha) = t^2 + x^2 + y^2 + z^2 = (t_1^2 + x_1^2 + y_1^2 + z_1^2)/4 \in \mathbb{Z}$. Máme teda $t_1^2 + x_1^2 + y_1^2 + z_1^2 \equiv 0 \mod 4$. Keďže t_1, x_1, y_1, $z_1 \in \mathbb{Z}$ a kvadratické zvyšky modulo 4 sú 0 alebo 1, tak máme dve možnosti:

- Platí $t_1^2 \equiv x_1^2 \equiv y_1^2 \equiv z_1^2 \equiv 0 \mod 4$. Z toho vieme, že každý z prvkov t_1, x_1, y_1, z_1 je kongruentný 0 alebo 2 modulo 4. V oboch prípadoch to však znamená, že každý z týchto prvkov je párne číslo, z čoho vyplýva, že t, x, y, $z \in \mathbb{Z}$.
- Platí $t_1^2 \equiv x_1^2 \equiv y_1^2 \equiv z_1^2 \equiv 1 \mod 4$. Odtiaľ vieme, že každý z prvkov t_1, x_1, y_1, z_1 je kongruentný 1 alebo 3 modulo 4. To tentokrát v oboch prípadoch znamená, že každý z týchto prvkov je nepárne číslo, z čoho vyplýva, že t, x, y, $z \in \frac{1}{2} + \mathbb{Z}$.

Začínali sme s ľubovoľným $\mathcal{O}'$ takým, že $\mathbb{Z}\langle i, j\rangle \subsetneq \mathcal{O}'$ a ukázali sme, že $\mathcal{O}'$ je Hurwitzov rád. Takže jediný rád, ktorý vlastne obsahuje Lipschitzov rád je Hurwitzov rád.

□

Z posledného tvrdenia priamo vidno, že Lipschitzov rád nie je maximálny, keďže je vlastne obsiahnutý v inom ráde. Naopak, Hurwitzov rád je maximálny, pretože inak by to nebol jediný rád, ktorý vlastne obsahuje Lipschitzov rád.

Dôsledok 3.17. *Lipschitzov rád nie je maximálny. Hurwitzov rád je maximálny.*

Poznámka. Pre porovnanie môžeme uviesť nasledujúcu paralelu: $\mathbb{Z}[\sqrt{-3}]$ je rád v $\mathbb{Q}(\sqrt{-3})$, ale tiež nie je maximálny. Podobne je však vlastne obsiahnutý v ráde $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, ktorý je známy ako Eisensteinove celé čísla. Paralela dokonca vysvetľuje označenie ω zo začiatku kapitoly. Pri Eisensteinových celých číslach značíme $\omega = \frac{-1+\sqrt{-3}}{2}$ a platí rovnosť $(2\omega + 1)^2 = -3$. Ak pre zmenu v Hurwitzovom ráde značíme $\omega = \frac{-1+i+j+k}{2}$, tak rovnako platí vzťah $(2\omega + 1)^2 = -3$, keďže $(i + j + k)^2 = -3$.

3.4 Rád v kvaterniónovej algebre $\left(\frac{-3,-1}{\mathbb{Q}}\right)$

Uvedieme si ešte jeden príklad rádu v kvaterniónovej algebre. Tentokrát sa presunieme do kvaterniónovej algebry $B = \left(\frac{-3,-1}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}\sqrt{-3} + \mathbb{Q}j + \mathbb{Q}\sqrt{-3}j$, kde $j^2 = -1$ a $\sqrt{-3}j = -j\sqrt{-3}$. To, prečo sme si vybrali túto kvaterniónovú algebru, a ako ju značíme, vyplýva z toho, ako budeme následne tieto poznatky aplikovať v kapitole číslo 5. Zaveďme ešte značenie ako pri Eisensteinových celých číslach, kde $\omega = (-1 + \sqrt{-3})/2$. Na začiatok ešte upozorníme, že v tejto sekcii značí ω niečo iné, ako v predchádzajúcej. Potom nasledujúcim spôsobom zadefinujeme rád v kvaterniónovej algebre B.

Definícia 3.18. *V kvaterniónovej algebre* $B = \left(\frac{-3,-1}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}\sqrt{-3} + \mathbb{Q}j + \mathbb{Q}\sqrt{-3}j$ *definujeme rád* $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega + \mathbb{Z}j + \mathbb{Z}\omega j$.

Opäť, rovnako ako pri Hurwitzovom ráde overíme, že je daná definícia rádu korektná. Potrebujeme ukázať, že mriežka $\mathcal{O} = \mathbb{Z}+\mathbb{Z}\omega+\mathbb{Z}j+\mathbb{Z}\omega j$ je uzavretá na násobenie, a teda sa naozaj jedná o rád v zmysle definície 3.2. Predstavme si, že násobíme dva prvky z $\mathcal{O}$. Buď nám pri násobení vyjdu rovno členy tvaru $1, \omega, j, \omega j$, ktoré samozrejme rádu patria, alebo nám vyjde niektorý z nasledujúcich členov tvaru $\omega^2, \omega^2 j, j\omega, j\omega j, \omega j\omega, \omega j\omega j$. Ak ukážeme, že tieto prvky patria $\mathcal{O}$, tak je to rád. Pre overenie, každý z týchto prvkov vyjadríme ako prvok z $\mathcal{O}$, pričom budeme využívať, že v algebre B platí $\sqrt{-3}j = -j\sqrt{-3}$, $j^2 = -1$. Takže máme:

- $\omega^2 = (\frac{-1+\sqrt{-3}}{2})^2 = \frac{1-2\sqrt{-3}-3}{4} = \frac{-1-\sqrt{-3}}{2} = \frac{1-\sqrt{-3}}{2} - 1 = -\omega - 1$,
- $\omega^2 j = (-\omega - 1)j = -\omega j - j$,
- $j\omega = j(\frac{-1+\sqrt{-3}}{2}) = \frac{-j+j\sqrt{-3}}{2} = \frac{-j-\sqrt{-3}j}{2} = (\frac{-1-\sqrt{-3}}{2})j = -\omega j - j$,
- $j\omega j = (-\omega j - j)j = \omega + 1$,
- $\omega j\omega = \omega(-\omega j - j) = -\omega^2 j - \omega j = -(-\omega j - j) - \omega j = j$,
- $\omega j\omega j = j^2 = -1$.

Znova platí, že sa na prvky rádu $\mathcal{O}$ môžeme pozerať dvoma spôsobmi. Buď si prvok α môžeme vyjadriť priamo z definície ako $\alpha = s + l\omega + mj + n\omega j$, kde už s, l, m, $n \in \mathbb{Z}$, alebo naopak, môžeme daný prvok vnímať ako prvok $B = \left(\frac{-3,-1}{\mathbb{Q}}\right)$, a teda písať $\alpha = t + x\sqrt{-3} + yj + z\sqrt{-3}j$, kde t, x, y, $z \in \mathbb{Q}$, a navyše ešte spĺňajú nejaké podmienky. Práve tieto podmienky charakterizujeme v nasledujúcej lemme.

Lemma 3.19. *Nech $\alpha \in \left(\frac{-3,-1}{\mathbb{Q}}\right)$, $\alpha = t + x\sqrt{-3} + yj + z\sqrt{-3}j$, kde t, x, y, $z \in \mathbb{Q}$. Potom platí, že $\alpha \in \mathbb{Z} + \mathbb{Z}\omega + \mathbb{Z}j + \mathbb{Z}\omega j$ práve vtedy, keď nastáva jedna z nasledujúcich možností:*

- *t, x, y, $z \in \mathbb{Z}$,*
- *t, $x \in \mathbb{Z}$, y, $z \in \frac{1}{2} + \mathbb{Z}$,*
- *t, $x \in \frac{1}{2} + \mathbb{Z}$, y, $z \in \mathbb{Z}$,*
- *t, x, y, $z \in \frac{1}{2} + \mathbb{Z}$.*

Dôkaz. Pre prvú implikáciu predpokladajme, že $\alpha \in \mathbb{Z} + \mathbb{Z}\omega + \mathbb{Z}j + \mathbb{Z}\omega j$, čo znamená $\alpha = s + l\omega + mj + n\omega j$ pre nejaké s, l, m, $n \in \mathbb{Z}$. Potom platí:

$$\begin{aligned}\alpha = s + l\omega + mj + n\omega j &= s + l\left(\frac{-1+\sqrt{-3}}{2}\right) + mj + n\left(\frac{-1+\sqrt{-3}}{2}\right)j \\ &= \left(s - \frac{l}{2}\right) + \left(\frac{l}{2}\right)\sqrt{-3} + \left(m - \frac{n}{2}\right)j + \left(\frac{n}{2}\right)\sqrt{-3}j.\end{aligned}$$

Ak n je párne číslo, tak koeficient $n/2$ pri $\sqrt{-3}j$ je celé číslo a rovnako aj koeficient $m - n/2$ pri j bude celé číslo. Naopak, ak n je nepárne číslo, tak oba koeficienty budú z $\frac{1}{2} + \mathbb{Z}$.

Úplne rovnakou úvahou vidíme, že ak l bude párne číslo, tak koeficient $l/2$ pri $\sqrt{-3}$ je zo $\mathbb{Z}$, a tým pádom aj koeficient $s - l/2 \in \mathbb{Z}$. Naopak, pre l nepárne budú oba koeficienty z $\frac{1}{2} + \mathbb{Z}$.

Dokopy sme tým ukázali, že ak prvok z rádu $\mathbb{Z} + \mathbb{Z}\omega + \mathbb{Z}j + \mathbb{Z}\omega j$ zapíšeme v tvare $t + x\sqrt{-3} + yj + z\sqrt{-3}j$, tak všetky koeficienty budú zo $\mathbb{Z}$ alebo $\frac{1}{2} + \mathbb{Z}$, a navyše bude platiť, že koeficienty t a x sú vždy rovnakého typu a rovnako aj koeficienty y a z.

Pre opačnú implikáciu nech $\alpha = t + x\sqrt{-3} + yj + z\sqrt{-3}j \in \left(\frac{-3,-1}{\mathbb{Q}}\right)$ a platí niektorá zo štyroch podmienok vymenovaných v znení lemmy. Potom môžeme spraviť úpravu:

$$\begin{aligned}\alpha &= t + x\sqrt{-3} + yj + z\sqrt{-3}j = (t+x) - x + x\sqrt{-3} + (y+z)j - zj + z\sqrt{-3}j \\ &= (t+x) + 2x\left(\frac{-1+\sqrt{-3}}{2}\right) + (y+z)j + 2z\left(\frac{-1+\sqrt{-3}}{2}\right)j \\ &= (t+x) + 2x\omega + (y+z)j + 2z\omega j.\end{aligned}$$

Keďže t, x, y, $z \in \frac{1}{2}\mathbb{Z}$, tak vieme rovno, že koeficienty $2x$ a $2z$ sú zo $\mathbb{Z}$. Ostáva ukázať, že aj koeficienty $t + x$ a $y + z$ tiež patria $\mathbb{Z}$. Ak to ukážeme, tak potom už nutne $\alpha \in \mathbb{Z} + \mathbb{Z}\omega + \mathbb{Z}j + \mathbb{Z}\omega j$. Vieme, že pre t a x platí, že buď sú obe zo $\mathbb{Z}$, a teda aj $t + x \in \mathbb{Z}$, alebo platí, že sú obe z $\frac{1}{2} + \mathbb{Z}$, potom ale opäť $t + x \in \mathbb{Z}$. Úplne analogicky je to aj v prípade $y + z$.

□

Tvrdenie 3.20. *Rád $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega + \mathbb{Z}j + \mathbb{Z}\omega j$ je v kvaterniónovej algebre $\left(\frac{-3,-1}{\mathbb{Q}}\right)$ maximálny.*

Dôkaz. Predpokladajme, že existuje rád $\mathcal{O}'$ v kvaterniónovej algebre $\left(\frac{-3,-1}{\mathbb{Q}}\right)$ taký, že $\mathcal{O} \subseteq \mathcal{O}'$. Vezmime prvok $\alpha \in \mathcal{O}'$, $\alpha = t + x\sqrt{-3} + yj + z\sqrt{-3}j$, kde t, x, y, $z \in \mathbb{Q}$.

Keďže $\mathcal{O}'$ je rád, tak podľa tvrdení 3.7 a 3.8 platí, že všetky prvky z $\mathcal{O}'$ majú celočíselnú stopu aj normu. Vieme, že prvky α, αj, $\alpha\omega$ a $\alpha\omega j$ sú určite všetky v ráde $\mathcal{O}'$. Potom dostávame:

- $Tr(\alpha) = 2t \in \mathbb{Z}$,
- $Tr(\alpha j) = Tr(tj + x\sqrt{-3}j - y - z\sqrt{-3}) = -2y \in \mathbb{Z}$,
- $Tr(\alpha\omega) = Tr(t(\frac{-1+\sqrt{-3}}{2}) + x\sqrt{-3}(\frac{-1+\sqrt{-3}}{2}) + yj(\frac{-1+\sqrt{-3}}{2}) + z\sqrt{-3}j(\frac{-1+\sqrt{-3}}{2}))$ $= 2(\frac{-t}{2} + \frac{-3x}{2}) = -t - 3x \in \mathbb{Z}$,
- $Tr(\alpha\omega j) = Tr(t(\frac{-1+\sqrt{-3}}{2})j + x\sqrt{-3}(\frac{-1+\sqrt{-3}}{2})j + yj(\frac{-1+\sqrt{-3}}{2})j +$ $z\sqrt{-3}j(\frac{-1+\sqrt{-3}}{2})j) = 2(\frac{y}{2} + \frac{-3z}{2}) = y - 3z \in \mathbb{Z}$,
- $N(\alpha) = N(t + x\sqrt{-3} + yj + z\sqrt{-3}j) = t^2 + 3x^2 + y^2 + 3z^2 \in \mathbb{Z}$.

Keďže $2t$, $-2y \in \mathbb{Z}$, tak z toho vieme odvodiť, že t, $y \in \frac{1}{2}\mathbb{Z}$. Následne, keď $-t - 3x \in \mathbb{Z}$ a my už vieme, že $t \in \frac{1}{2}\mathbb{Z}$, tak z toho priamo dostávame aj $3x \in \frac{1}{2}\mathbb{Z}$, z čoho plynie $x \in \frac{1}{6}\mathbb{Z}$. Obdobne to ukážeme aj pre $y - 3z \in \mathbb{Z}$ a dostaneme $z \in \frac{1}{6}\mathbb{Z}$.

Vďaka práve zistenému označme $t_1 = 2t$, $y_1 = 2y$, $x_1 = 6x$ a $z_1 = 6z$, kde už vieme, že t_1, x_1, y_1, $z_1 \in \mathbb{Z}$. Potom z poslednej podmienky plynie, že:

$$t^2+3x^2+y^2+3z^2 \in \mathbb{Z} \Longrightarrow \frac{t_1^2}{4}+\frac{3x_1^2}{36}+\frac{y_1^2}{4}+\frac{3z_1^2}{36} \in \mathbb{Z} \Longrightarrow \frac{3t_1^2+x_1^2+3y_1^2+z_1^2}{12} \in \mathbb{Z}.$$

Z toho potom rovno plynie nasledujúce:

$$3t_1^2 + x_1^2 + 3y_1^2 + z_1^2 \equiv 0 \mod 12 \Longrightarrow x_1^2 + z_1^2 \equiv 0 \mod 3.$$

Keďže modulo 3 máme iba kvadratické zvyšky 0 a 1, tak platí, že potom nutne x_1, $y_1 \equiv 0 \mod 3$. To znamená, že napríklad x_1 môžeme zapísať aj v tvare $x_1 = 3x_2$, kde je $x_2 \in \mathbb{Z}$. Dosadením do rovnice $x_1 = 6x$ získame $3x_2 = 6x$ a po skrátení $x_2 = 2x$. To ale znamená, že x vieme vyjadriť ako $x_2/2$, kde $x_2 \in \mathbb{Z}$, a teda z toho môžeme usúdiť, že $x \in \frac{1}{2}\mathbb{Z}$. Úplne analogickou úvahou dostávame aj $z \in \frac{1}{2}\mathbb{Z}$. Dokopy teda zatiaľ vieme, že pre všetky koeficienty t, x, y, z platí, že patria $\frac{1}{2}\mathbb{Z}$.

Vyššie sme ukázali, že $-t - 3x \in \mathbb{Z}$. Z toho ale priamo plynie, že buď oba prvky t aj x sú zo $\mathbb{Z}$ alebo oba z $\frac{1}{2}\mathbb{Z}$. A vďaka $y - 3z \in \mathbb{Z}$ rovnako aj pre y a z.

Ukázali sme, že pre každý prvok $\alpha \in \mathcal{O}'$, $\alpha = t + x\sqrt{-3} + yj + z\sqrt{-3}j$ platí niektorá z podmienok z lemmy 3.19, a teda $\alpha \in \mathbb{Z} + \mathbb{Z}\omega + \mathbb{Z}j + \mathbb{Z}\omega j$. To ale znamená, že z $\mathcal{O} \subseteq \mathcal{O}'$ dostávame $\mathcal{O} = \mathcal{O}'$. Z čoho vidíme, že rád $\mathcal{O}$ je maximálny. □

Následne ešte opäť dokážeme, ako vyzerá grupa jednotiek v tomto ráde. Dôkaz bude miestami podobný ako pri Hurwitzovom ráde.

Tvrdenie 3.21. *Grupa jednotiek rádu* $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega + \mathbb{Z}j + \mathbb{Z}\omega j$ *je* $\mathcal{O}^\times = \{\pm 1, \pm j, \pm\omega, \pm\omega^2, \pm\omega j, \pm\omega^2 j\}$*, čiže grupa rádu 12.*

Dôkaz. Predpokladajme, že $\alpha \in \mathcal{O}^\times$. Existuje teda $\beta \in \mathcal{O}$ taká, že platí $\alpha\beta = 1$. Nech platí $\alpha = t + x\sqrt{-3} + yj + z\sqrt{-3}j$, $\beta = s + l\sqrt{-3} + mj + n\sqrt{-3}j$. Potom podľa lemmy 3.19 vieme, že t, x, y, z, s, l, m, $n \in \frac{1}{2}\mathbb{Z}$. Zaveďme značenie $t_1 = 2t$ a analogicky pre všetkých sedem zvyšných neznámych. Vďaka tomu, že patria $\frac{1}{2}\mathbb{Z}$, tak potom už nutne t_1, x_1, y_1, z_1, s_1, l_1, m_1, $n_1 \in \mathbb{Z}$.

Vráťme sa k rovnosti $\alpha\beta = 1$ a aplikujme na obe strany normu. Vďaka multiplikativite dostaneme $N(\alpha)N(\beta) = 1$. Teraz môžeme obe normy vyjadriť a získame:

$$\begin{aligned} 1 &= N(\alpha)N(\beta) = N(t + x\sqrt{-3} + yj + z\sqrt{-3}j)N(s + l\sqrt{-3} + mj + n\sqrt{-3}j) = \\ &= (t^2 + 3x^2 + y^2 + 3z^2)(s^2 + 3l^2 + m^2 + 3n^2) = \\ &= \left(\frac{t_1^2 + 3x_1^2 + y_1^2 + 3z_1^2}{4}\right)\left(\frac{s_1^2 + 3l_1^2 + m_1^2 + 3n_1^2}{4}\right). \end{aligned}$$

Po prenásobení dostávame rovnicu $16 = (t_1^2+3x_1^2+y_1^2+3z_1^2)(s_1^2+3l_1^2+m_1^2+3n_1^2)$, kde všetky neznáme sú už celočíselné. Každá zo zátvoriek predstavuje kladné celé číslo, a teda máme 5 možností ako 16 rozložiť na súčin:

- Platí $t_1^2 + 3x_1^2 + y_1^2 + 3z_1^2 = 1$, $s_1^2 + 3l_1^2 + m_1^2 + 3n_1^2 = 16$. To znamená, že t_1 alebo y_1 sú rovné ± 1, zatiaľ čo $x_1 = z_1 = 0$. Z toho plynie, že $x = z = 0$ a jedna z neznámych t, y je rovná $\pm 1/2$ a druhá 0. To je ale spor s lemmou 3.19.

- Platí $t_1^2 + 3x_1^2 + y_1^2 + 3z_1^2 = 2$, $s_1^2 + 3l_1^2 + m_1^2 + 3n_1^2 = 8$. Potom jediná možnosť je $t_1 = y_1 = \pm 1$ a $x_1 = z_1 = 0$. Odtiaľ $t = y = \pm 1/2$, $x = z = 0$, čo je opäť spor s lemmou 3.19.

- Ďalšie dve možnosti by boli, že by sme hodnoty jednotlivých zátvoriek z predchádzajúcich dvoch bodov prehodili. To by však viedlo k analogickým úvahám pre neznáme s, l, m, n, ktoré by viedli k sporu.

- Platí $t_1^2 + 3x_1^2 + y_1^2 + 3z_1^2 = 4$, $s_1^2 + 3l_1^2 + m_1^2 + 3n_1^2 = 4$. Potom sú dve možnosti ako to docieliť:

  - Platí, že t_1 alebo y_1 je rovné ± 2 a zvyšné sú nulové. Z toho získame $\alpha = t = \pm 1$ alebo $\alpha = yj = \pm j$.
  - Platí, že $t_1 = x_1 = \pm 1$, $y_1 = z_1 = 0$. Z toho získame $\alpha = t + x\sqrt{-3} = \frac{\pm 1 \pm \sqrt{-3}}{2}$. Tieto prvky môžeme popísať ako $\pm\omega$ a $\pm\omega^2$. Alebo naopak $t_1 = x_1 = 0$, $y_1 = z_1 = \pm 1$. Z toho máme $\alpha = yj + z\sqrt{-3}j = \frac{\pm j \pm \sqrt{-3}j}{2}$. Tieto prvky zas môžeme popísať ako $\pm\omega j$ a $\pm\omega^2 j$. Keďže podľa lemmy 3.19 potrebujeme, aby t a x respektíve y a z boli rovnakého typu, tak toto sú jediné možnosti, ktoré prichádzali do úvahy.

Určili sme prvky, ktoré prichádzajú do úvahy, že by mohli byť jednotkami. Ostáva ako posledný krok overiť, že všetky tieto prvky $\{\pm 1, \pm j, \pm\omega, \pm\omega^2, \pm\omega j, \pm\omega^2 j\}$ sú naozaj jednotky. Rovno vidíme, že prvky j a $-j$ sú si navzájom inverzmi, keďže $j^2 = -1$. Zároveň vieme, že $(\pm\omega)(\pm\omega^2) = (\pm\omega^2)(\pm\omega) = \omega^3 = 1$, a teda aj tieto prvky sú si navzájom inverzmi. Využitím vzťahov, ktoré sme odvodili priamo za definíciou 3.18 vidíme, že aj $(\pm\omega j)(\mp\omega j) = -\omega j \omega j = 1$ a $(\pm\omega^2 j)(\mp\omega^2 j) = -\omega^2 j \omega^2 j = -(-\omega j - j)(\omega^2 j) = -(j\omega)(\omega^2 j) = -j^2 = 1$. Všetky tieto prvky sú naozaj jednotkami a platí $\mathcal{O}^\times = \{\pm 1, \pm j, \pm\omega, \pm\omega^2, \pm\omega j, \pm\omega^2 j\}$.

□

4. Konečné podgrupy $\mathbb{H}^\times$

V tejto kapitole budeme postupne smerovať k úplnej klasifikácii konečných podgrúp $\mathbb{H}^\times$, pričom $\mathbb{H}^\times$ vnímame ako grupu vzhľadom k násobeniu kvaterniónov. Táto klasifikácia bude následne kľúčová pri klasifikácii konečných grúp jednotiek v rádoch v hamiltonovských kvaterniónoch. V celej kapitole pospájame niektoré časti z knihy Quaternion algebras od J. Voighta [11]. Uvedieme však kompletné podrobnejšie výpočty a dôkazy, ktoré sa v knihe nenachádzajú.

Predpokladajme teda, že $\Gamma \subseteq \mathbb{H}^\times$ je konečná podgrupa. Z definície normy 1.4 plynie, že norma každého nenulového kvaterniónu je kladné reálne číslo, a teda $N(\Gamma) \subseteq \mathbb{R}^+$. Následne vďaka multiplikativite normy 1.5 dostávame, že $N(\Gamma)$ je konečná podgrupa $\mathbb{R}^+$. Čo ale rovno znamená, že $N(\Gamma) = \{1\}$. Keďže sme dostali, že každý prvok z Γ má normu 1, tak platí, že Γ je vlastne konečná podgrupa $\mathbb{H}^1$. Naša úloha sa tým pádom zmenila na to, že chceme klasifikovať konečné podgrupy $\mathbb{H}^1$.

4.1 Rotácie v $\mathbb{R}^3$ a kvaternióny

Na chvíľu odbočíme od našej hlavnej úlohy a pozrieme sa, ako súvisia rotácie v $\mathbb{R}^3$ a kvaternióny. Budeme postupovať podľa knihy The four pillars of geometry od J. Stillwella [10, Kapitola 7.6] a podľa Quaternion algebras od J.Voighta [11, Kapitola 2.4].

Každá rotácia v $\mathbb{R}^3$ sa dá popísať pomocou dvoch vecí: os, okolo ktorej rotujeme a veľkosť uhla, o ktorý daný priestor rotujeme. Inak povedané, na popis rotácie v $\mathbb{R}^3$ nám stačí uhol $\theta \in [0, 2\pi]$ a jednotkový vektor (l,m,n), ktorý definuje os rotácie.

Tvrdenie 4.1. *Nech $q \in \mathbb{H}^1\backslash\{\pm 1\}$, $q = t + xi + yj + zk$. Potom existuje jednoznačne určený uhol $\theta \in (0, 2\pi)$ a $l, m, n \in \mathbb{R}$ také, že $l^2 + m^2 + n^2 = 1$ a zároveň platí $q = \cos(\theta/2) + (li + mj + nk)\sin(\theta/2)$.*

Dôkaz. Majme $q = t + xi + yj + zk$, $q \in \mathbb{H}^1\backslash\{\pm 1\}$. Keďže $q \in \mathbb{H}^1$, tak dostávame $N(q) = t^2 + x^2 + y^2 + z^2 = 1$. Chceme, aby pre nejaké θ a l, m, n platil vzťah $q = t + xi + yj + zk = \cos(\theta/2) + (li + mj + nk)\sin(\theta/2)$. To znamená, že sa musia rovnať reálne časti kvaterniónov, a teda $t = \cos(\theta/2)$. Keďže $t \in (-1,1)$, tak vždy existuje jednoznačne určený uhol $\theta \in (0, 2\pi)$, ktorý spĺňa túto rovnosť.

Vieme, že platí $t^2 = \cos^2(\theta/2)$. Spojením $t^2 + x^2 + y^2 + z^2 = 1$ a známej identity $\cos^2(\theta/2) + \sin^2(\theta/2) = 1$, dostávame $x^2 + y^2 + z^2 = \sin^2(\theta/2)$. Odkiaľ $\sin(\theta/2) = \pm\sqrt{x^2 + y^2 + z^2}$, ale keďže $\theta/2 \in (0,\pi)$, tak na tomto intervale je sínus kladný a máme $\sin(\theta/2) = \sqrt{x^2 + y^2 + z^2} > 0$.

Pre rovnosť imaginárnych častí kvaterniónov potrebujeme, aby platil nasledujúci vzťah $xi + yj + zk = (li + mj + nk)\sin(\theta/2)$. Z toho vieme vyjadriť $(li + mj + nk) = (xi + yj + zk)/\sin(\theta/2) = (xi + yj + zk)/\sqrt{x^2 + y^2 + z^2}$. Získavame jednoznačne určené $l = x/\sqrt{x^2 + y^2 + z^2}$, $m = y/\sqrt{x^2 + y^2 + z^2}$ a $n = z/\sqrt{x^2 + y^2 + z^2}$. Jednoducho vieme overiť, že naozaj platí $l^2 + m^2 + n^2 = 1$.

Ukázali sme, že každý $q \in \mathbb{H}^1 \backslash \{\pm 1\}$ sa dá zapísať v požadovanom tvare, pričom uhol $\theta \in (0, 2\pi)$ aj trojica (l, m, n) sú určené jednoznačne.

□

Z posledného tvrdenia vyplýva, že každý kvaternión $q \in \mathbb{H}^1 \backslash \{\pm 1\}$ jednoznačne určuje uhol $\theta \in (0, 2\pi)$ a jednotkový vektor (l, m, n). Kvaternióny 1 a -1 sú špeciálne a môžeme ich chápať tak, že im postupne prislúchajú uhly 0 a 2π, keďže $1 = \cos(0/2)$ a $-1 = \cos(2\pi/2)$. Intuitívne už vidíme, že jednotkový kvaternión nesie dostatok informácií na to, aby v nejakom zmysle mohol popisovať rotáciu v $\mathbb{R}^3$. Teraz zadefinujeme presné zobrazenie, pomocou ktorého tento vzťah formálne popíšeme.

Definícia 4.2. *Pre $q \in \mathbb{H}^1$ definujeme zobrazenie $\phi_q : \mathbb{H}^0 \to \mathbb{H}^0$ s predpisom $\phi_q(p) = qpq^{-1}$.*

Ak vezmeme ľubovoľný jednotkový kvaternión $q = t + xi + yj + zk$, kde $t^2 + x^2 + y^2 + z^2 = 1$ a $p = ai + bj + ck$, tak na overenie korektnosti definície stačí dosadiť a zrátať súčin qpq^{-1}. Po vyčíslení nám vyjde kvaternión s nulovou reálnou časťou, a teda $qpq^{-1} \in \mathbb{H}^0$.

Poznámka. Kvaternióny q a $-q$ určujú rovnaké zobrazenie, keďže platí $\phi_q(p) = qpq^{-1} = (-q)p(-q)^{-1} = \phi_{-q}(p)$.

Veta 4.3 (reprezentácia rotácie v $\mathbb{R}^3$ kvaterniónom)**.** *Nech $q \in \mathbb{H}^1 \backslash \{\pm 1\}$ je tvaru $q = \cos(\theta/2) + (li + mj + nk)\sin(\theta/2)$, kde $l^2 + m^2 + n^2 = 1$ a $\theta \in (0, 2\pi)$. Potom zobrazenie ϕ_q z definície 4.2 je rotácia v $\mathbb{R}^3$ o uhol θ okolo osi, ktorá je určená jednotkovým vektorom (l,m,n). Zobrazenia ϕ_1 a ϕ_{-1} určujú identitu.*

Dôkaz. Zobrazenie ϕ_q je definované na $\mathbb{H}^0$. Lenže kvaternióny z $\mathbb{H}^0$, ktoré sú tvaru $li + mj + nk$, môžeme stotožniť s vektormi (l, m, n) v $\mathbb{R}^3$. Potom zobrazenie ϕ_q môžeme vnímať ako zobrazenie v $\mathbb{R}^3$. To, že ϕ_1 a ϕ_{-1} určujú identitu, vidíme priamo z definície 4.2. Ďalej predpokladajme, že $q \in \mathbb{H}^1 \backslash \{\pm 1\}$, $q = \cos(\theta/2) + (li + mj + nk)\sin(\theta/2)$, kde $l^2 + m^2 + n^2 = 1$.

Označme $i' = li + mj + nk$, potom $q = \cos(\theta/2) + i'\sin(\theta/2)$. Nájdeme kvaternión $j' = ai + bj + ck \in \mathbb{H}^1$ taký, že vektor (a, b, c) je v $\mathbb{R}^3$ kolmý na vektor (l, m, n). Potom vieme, že platí $a^2 + b^2 + c^2 = 1$ a $al + bm + cn = 0$. Využitím týchto vzťahov ukážeme, že pre i' a j' platí $(i')^2 = (j')^2 = -1$ a $j'i' = -i'j'$:

- $(i')^2 = (li + mj + nk)(li + mj + nk) = -l^2 + lmk - lnj - mlk - m^2 + mni + nlj - nmi - n^2 = -(l^2 + m^2 + n^2) = -1$,
- $(j')^2 = (ai + bj + ck)(ai + bj + ck) = -a^2 + abk - acj - bak - b^2 + bci + caj - cbi - c^2 = -(a^2 + b^2 + c^2) = -1$,
- $j'i' = (ai + bj + ck)(li + mj + nk) = -al + amk - anj - blk - bm + bni + clj - cmi - cn = -(al + bm + cn) + (bn - cm)i + (cl - an)j + (am - bl)k = (bn - cm)i + (cl - an)j + (am - bl)k$,
- $-i'j' = -(li + mj + nk)(ai + bj + ck) = al + amk - anj - blk + bm + bni + clj - cmi + cn = (al + bm + cn) + (bn - cm)i + (cl - an)j + (am - bl)k = (bn - cm)i + (cl - an)j + (am - bl)k$.

Zadefinujme ešte $k' = i'j' = (-bn + cm)i + (-cl + an)j + (-am + bl)k$. Vieme, že $q = \cos(\theta/2) + i' \sin(\theta/2)$, čiže $q^{-1} = \overline{q}/N(q) = \cos(\theta/2) - i' \sin(\theta/2)$. S využitím všetkých vzťahov, ktoré sme doteraz ukázali, a súčtových vzorcov, sa teraz pozrieme, ako vyzerá zobrazenie ϕ_q aplikované na i', j' a k':

- $\phi_q(i') = qi'q^{-1} = (\cos(\theta/2) + i' \sin(\theta/2))i'(\cos(\theta/2) - i' \sin(\theta/2)) = \cos^2(\theta/2)i' - \cos(\theta/2)\sin(\theta/2)(i')^2 + \cos(\theta/2)\sin(\theta/2)(i')^2 - \sin^2(\theta/2)(i')^3 = (\cos^2(\theta/2) + \sin^2(\theta/2))i' = i'$,
- $\phi_q(j') = qj'q^{-1} = (\cos(\theta/2) + i' \sin(\theta/2))j'(\cos(\theta/2) - i' \sin(\theta/2)) = \cos^2(\theta/2)j' - \cos(\theta/2)\sin(\theta/2)j'i' + \cos(\theta/2)\sin(\theta/2)i'j' - \sin^2(\theta/2)i'j'i' = (\cos^2(\theta/2) - \sin^2(\theta/2))j' + 2\cos(\theta/2)\sin(\theta/2)i'j' = \cos(\theta)j' + \sin(\theta)k'$,
- $\phi_q(k') = qk'q^{-1} = (\cos(\theta/2) + i' \sin(\theta/2))k'(\cos(\theta/2) - i' \sin(\theta/2)) = \cos^2(\theta/2)k' - \cos(\theta/2)\sin(\theta/2)k'i' + \cos(\theta/2)\sin(\theta/2)i'k' - \sin^2(\theta/2)i'k'i' = (\cos^2(\theta/2) - \sin^2(\theta/2))k' - 2\cos(\theta/2)\sin(\theta/2)j' = \cos(\theta)k' - \sin(\theta)j'$.

Keď sa na prvky i', j' a k' pozrieme ako na vektory v $\mathbb{R}^3$, tak postupne dostaneme $(l, m, n), (a,b,c)$ a $(cm - bn, an - cl, bl - am)$. Vektory (l, m, n) a (a,b,c) boli zvolené tak, aby na seba boli kolmé. Zároveň výpočtom štandardného skalárneho súčinu vieme overiť, že aj vektor $(cm - bn, an - cl, am - bl)$ je na nich kolmý.

To znamená, že prvky i', j' a k', prevedené na vektory $\mathbb{R}^3$, tvoria ortogonálnu bázu $\mathbb{R}^3$. Potom podľa výpočtov je matica zobrazenia ϕ_q vzhľadom k tejto báze:

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

Vieme, že Q je matica rotácie v $\mathbb{R}^3$ o uhol θ okolo prvej súradnicovej osi. V našom prípade prvú súradnicovú os predstavoval kvaternión i', a teda bola daná jednotkovým vektorom (l, m, n). Dokázali sme, že zobrazenie ϕ_q odpovedá rotácii v $\mathbb{R}^3$ o uhol θ okolo osi danej vektorom (l, m, n).

□

4.2 Konečné podgrupy $SO(3)$

V tejto podkapitole ukážeme, prečo bol v kontexte klasifikácie konečných podgrúp $\mathbb{H}^1$ dôležitý súvis kvaterniónov a rotácií v $\mathbb{R}^3$. Z minulej sekcie vieme, že každý pár $\pm q$ má priradené zobrazenie, ktoré určuje rotáciu v $\mathbb{R}^3$. Formálne tento fakt zhrnieme v ďalšej vete. Pripomeňme, že $SO(3)$ je grupa rotácií v $\mathbb{R}^3$ vzhľadom na skladanie zobrazení a $\mathbb{H}^1$ tvorí grupu vzhľadom na násobenie kvaterniónov.

Veta 4.4. *Zobrazenie $\psi : \mathbb{H}^1 \to SO(3)$ definované predpisom $\psi(q) = \phi_q$ (pričom ϕ_q je zobrazenie z definície 4.2) je homomorfizmus, ktorý je na a* Ker $\psi = \{\pm 1\}$.

Dôkaz. Ako prvú vec si dokážeme, že dané zobrazenie predstavuje homomorfizmus grúp. To znamená, že chceme ukázať, že pre všetky q_1, $q_2 \in \mathbb{H}^1$ platí $\psi(q_1 q_2) = \psi(q_1) \circ \psi(q_2)$. Tento vzťah vieme odvodiť využitím definícií zobrazení ϕ, ψ a dosadením ľubovoľného $p \in \mathbb{H}^0$:

$$\psi(q_1q_2)(p) = \phi_{q_1q_2}(p) = (q_1q_2)p(q_1q_2)^{-1} = q_1q_2pq_2^{-1}q_1^{-1} = q_1(q_2pq_2^{-1})q_1^{-1}$$
$$= \phi_{q_1}(q_2pq_2^{-1}) = \phi_{q_1} \circ \phi_{q_2}(p) = \psi(q_1) \circ \psi(q_2)(p)$$

Predpokladajme, že $q \in \text{Ker } \psi$. Potom vieme, že $\psi(q) = \phi_q$ je identita. Podľa vety 4.3 je pre $q \neq \pm 1$ zobrazenie ϕ_q rotácia o uhol z intervalu $(0, 2\pi)$, čo nevyhovuje. Naopak pre $q = \pm 1$ to bude identické zobrazenie. Ukázali sme, že $\text{Ker } \psi = \{\pm 1\}$.

Každý netriviálny prvok $SO(3)$ je rotácia ρ v $\mathbb{R}^3$, ktorá sa dá popísať uhlom $\theta \in (0,2\pi)$ a jednotkovým vektorom (l,m,n). Pre každú takúto rotáciu ρ teda existuje príslušný kvaternión $q = \cos(\theta/2) + (li + mj + nk)\sin(\theta/2)$, $q \in \mathbb{H}^1$. Potom podľa vety 4.3 je to hľadaný vzor, pre ktorý platí $\psi(q) = \phi_q = \rho$. Preto je dané zobrazenie na.

□

Z 1. vety o izomorfizme dostávame nasledujúci dôsledok, ktorý môžeme chápať tak, že máme korešpondenciu medzi jednotkovým kvaterniónovým párom $\pm q$, $q = \cos(\theta/2) + (li + mj + nk)\sin(\theta/2)$ a rotáciou v $\mathbb{R}^3$ o uhol θ okolo osi danej vektorom (l,m,n).

Dôsledok 4.5. *Platí izomorfizmus* $\mathbb{H}^1/\{\pm 1\} \simeq SO(3)$.

Vďaka dôsledku vidíme, že na to, aby sme klasifikovali konečné podgrupy $\mathbb{H}^1/\{\pm 1\}$, nám stačí klasifikovať konečné podgrupy $SO(3)$. To je už známy problém, a klasifikáciu spolu s dôkazom môžeme nájsť napríklad v článku Classifying the finite subgroups of $SO(3)$, Hong Thien An Bui [2, Theorem 9.1.].

Veta 4.6 (konečné podgrupy $SO(3)$)**.** *Každá konečná podgrupa* $SO(3)$ *je jedného z nasledujúcich typov:*

- *T: tetrahedrálna grupa $\simeq A_4$ rádu 12 (grupa symetrií štvorstenu),*
- *O: oktahedrálna grupa $\simeq S_4$ rádu 24 (grupa symetrií osemstenu),*
- *I: ikosahedrálna grupa $\simeq A_5$ rádu 60 (grupa symetrií dvadsaťstenu),*
- *D_n: dihedrálna grupa rádu $2n$ (grupa symetrií pravidelného n-uholníka),*
- *C_n: cyklická grupa rádu n.*

4.3 Konečné podgrupy $\mathbb{H}^1$

Predchádzajúcu podkapitolu sme ukončili úplnou klasifikáciou konečných podgrúp $SO(3)$. V tejto časti prejdeme postupne jednotlivé možnosti z vety 4.6, a každú z podgrúp charakterizujeme a popíšeme ju ako podgrupu $\mathbb{H}^1/\{\pm 1\}$, čiže jej jednotlivé prvky prevedieme do reči kvaterniónov.

Ďalej si musíme uvedomiť, že máme prirodzený homomorfizmus medzi $\mathbb{H}^1$ a $\mathbb{H}^1/\{\pm 1\}$, ktorý je definovaný tak, že prvok q aj prvok $-q$ posiela na kvaterniónový pár $\pm q$. Pričom platí, že ak by Γ bola konečná podgrupa $\mathbb{H}^1$, tak jej obraz musí byť konečná podgrupa v $\mathbb{H}^1/\{\pm 1\}$. To znamená, že ak postupne charakterizujeme všetky konečné podgrupy $\mathbb{H}^1/\{\pm 1\}$ a pozrieme sa aký mohli mať vzor v $\mathbb{H}^1$, tak týmto spôsobom získame všetky konečné podgrupy $\mathbb{H}^1$.

4.3.1 Binárna tetrahedrálna grupa

Prvá z možností, ktorú rozoberieme je, že ako podgrupu $SO(3)$ máme tetrahedrálnu grupu T. Tento prípad je sčasti obsiahnutý v knihe The four pillars of geometry od J. Stillwella [10, Kapitola 7.7].

Definícia 4.7 (tetrahedrálna grupa)**.** Tetrahedrálna grupa T *je grupa rotačných symetrií pravidelného štvorstena.*

Tvrdenie 4.8 (prvky tetrahedrálnej grupy)**.** *Rotačné symetrie pravidelného štvorstena, a teda prvky tetrahedrálnej grupy sú:*

- *identita,*
- *3 rotácie o uhol π okolo osi spájajúcej stredy dvoch protiľahlých hrán štvorstena,*
- *4 rotácie o uhol $2\pi/3$ okolo osi spájajúcej vrchol štvorstena a stred protiľahlej steny štvorstena,*
- *4 rotácie o uhol $4\pi/3$ okolo osi spájajúcej vrchol štvorstena a stred protiľahlej steny štvorstena.*

Dôkaz. Najprv si uvedomíme, že rád tetrahedrálnej grupy je 12. Predstavme si, že máme pred sebou položený pravidelný štvorsten a zafixujme si pozíciu jednej jeho steny a na nej jednej konkrétnej hrany. Potom máme 4 spôsoby, ktorú stenu štvorstenu dať na zafixovanú pozíciu a 3 spôsoby, ktorú hranu na danej stene nastaviť na zafixovanú pozíciu hrany. Zároveň týmto už bude celá rotácia definovaná, ak chceme, aby sa štvorsten zobrazil presne na ten pôvodný. Znamená to, že máme $4 \cdot 3 = 12$ rotačných symetrií pravidelného štvorstena.

Teraz nám stačí popísať týchto 12 symetrií. Prvou z nich bude triviálna rotácia, teda identita. Následne existuje 11 netriviálnych rotácií, ktoré sú definované osou rotácie a uhlom. Máme dve možnosti, ako môže rotácia vyzerať:

- Rotácia o uhol π okolo osi spájajúcej stredy dvoch protiľahlých hrán štvorstena. Existujú 3 takéto osi, a teda tri rotácie tohto typu.
- Rotácia o uhol $2\pi/3$ alebo $4\pi/3$ okolo osi spájajúcej vrchol štvorstena a stred protiľahlej steny štvorstena. Existujú 4 takéto osi, a teda dokopy 8 rotácií tohto typu.

Vieme, že prvý typ rotácie prehadzuje medzi sebou všetky štyri vrcholy, zatiaľ čo druhý typ rotácie jeden vrchol fixuje a prehadzuje zvyšné tri. Z toho plynie, že všetkých 11 rotácií je rôznych a my sme našli všetky prvky tetrahedrálnej grupy. □

Teraz máme definované prvky tetrahedrálnej grupy ako podgrupy $SO(3)$. V minulej sekcii sme vo vetách 4.3 a 4.4 popísali korešpondenciu medzi rotáciou v $\mathbb{R}^3$ o uhol θ okolo osi danej (l,m,n) a kvaterniónovým párom $\pm q$, kde $q = \cos(\theta/2) + (li + mj + nk)\sin(\theta/2)$. Využijeme izomorfizmus $\mathbb{H}^1/\{\pm 1\} \simeq SO(3)$ z dôsledku 4.5 a popíšeme prvky tetrahedrálnej grupy ako odpovedajúce kvaterniónové páry v $\mathbb{H}^1/\{\pm 1\}$.

Vezmime si pravidelný štvorsten, ktorého ťažiskom bude počiatok súradnicovej sústavy $(0,0,0)$ a jeho vrcholy budú mať súradnice (1,1,1), $(1,-1,-1)$, $(-1,1,-1)$ a $(-1,-1,1)$.

Identita: Identickej rotácii vždy odpovedá kvaterniónový pár ± 1.

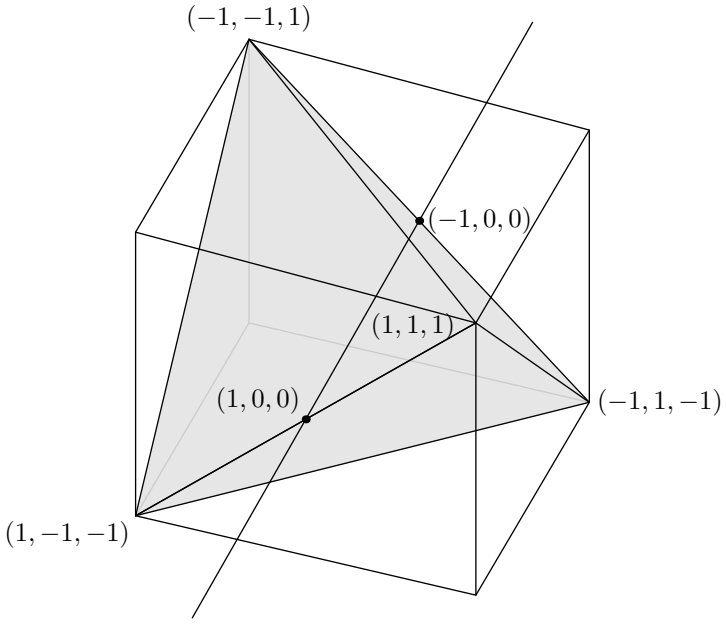
Rotácia okolo osi spájajúcej stredy protiľahlých hrán štvorstena o π:

Vďaka súradniciam, ktoré sme si zaviedli, vieme vyrátať, že stredy hrán nášho štvorstena majú súradnice $(\pm 1,0,0)$, $(0, \pm 1,0)$, $(0,0, \pm 1)$. Takže tri osi spájajúce stredy protiľahlých hrán vieme určiť napríklad jednotkovými vektormi (1,0,0), (0,1,0) a (0,0,1). Jednu z týchto troch osí môžeme vidieť na obrázku 4.1.

Keďže teraz máme už každú z rotácií popísanú jednotkovým vektorom a uhlom π, tak sa poďme pozrieť, aké kvaterniónové páry im odpovedajú. Stačí iba do vzťahu $q = \cos(\theta/2) + (li + mj + nk)\sin(\theta/2)$ dosadiť za θ uhol rotácie a za (l,m,n) nejaký jednotkový vektor, ktorý definuje os rotácie. Vždy týmto výpočtom dostaneme iba jeden kvaternión, ale vieme, že samotnej rotácií odpovedá kvaterniónový pár. Druhý z kvaterniónov by sme získali, ak by sme za vektor (l,m,n) dosadili opačný jednotkový vektor, ktorý definuje os rotácie.

Os rotácie	Uhol rotácie	Dosadenie	Kvaterniónový pár
(1,0,0)	π	$\cos\frac{\pi}{2} + (1i + 0j + 0k)\sin\frac{\pi}{2}$	$\pm i$
(0,1,0)	π	$\cos\frac{\pi}{2} + (0i + 1j + 0k)\sin\frac{\pi}{2}$	$\pm j$
(0,0,1)	π	$\cos\frac{\pi}{2} + (0i + 0j + 1k)\sin\frac{\pi}{2}$	$\pm k$

Ukázali sme, že rotáciám okolo osi spájajúcej stredy protiľahlých hrán štvorstena o uhol π odpovedajú kvaterniónové páry $\pm i, \pm j$ a $\pm k$.

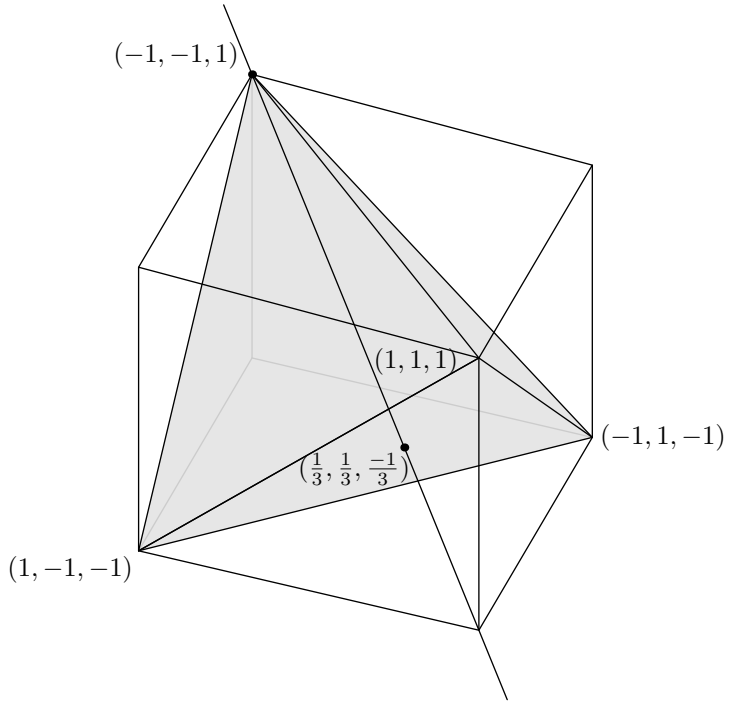


Obr. 4.1: Ukážka osi rotácie spájajúcej stredy protiľahlých hrán štvorstena.

Rotácia okolo osi spájajúcej vrchol štvorstena a stred protiľahlej steny štvorstena o $2\pi/3$ alebo $4\pi/3$:

Vďaka zavedeným súradniciam vieme vyrátať stredy jednotlivých stien štvorstena: $(\frac{1}{3},\frac{1}{3},\frac{-1}{3})$,$(\frac{-1}{3},\frac{1}{3},\frac{1}{3})$, $(\frac{1}{3},\frac{-1}{3},\frac{1}{3})$ a $(\frac{-1}{3},\frac{-1}{3},\frac{-1}{3})$. Keďže vieme aj súradnice vrcholov, tak vieme určiť vektory, ktoré definujú jednotlivé osi rotácií. Následne tieto vektory ešte vynormujeme a dostávame: $(\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}})$,$(\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$, $(\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$ a $(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})$. Opäť rovnakým spôsobom určíme prislúchajúce kvaterniónové páry.

Os rotácie	Uhol rotácie	Dosadenie	Kvaterniónový pár
$(\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{1}{\sqrt{3}}(-i-j+k)\sin\frac{\pi}{3}$	$\pm\frac{1-i-j+k}{2}$
$(\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{1}{\sqrt{3}}(i-j-k)\sin\frac{\pi}{3}$	$\pm\frac{1+i-j-k}{2}$
$(\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{1}{\sqrt{3}}(-i+j-k)\sin\frac{\pi}{3}$	$\pm\frac{1-i+j-k}{2}$
$(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{1}{\sqrt{3}}(i+j+k)\sin\frac{\pi}{3}$	$\pm\frac{1+i+j+k}{2}$
$(\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{1}{\sqrt{3}}(-i-j+k)\sin\frac{2\pi}{3}$	$\pm\frac{-1-i-j+k}{2}$
$(\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{1}{\sqrt{3}}(i-j-k)\sin\frac{2\pi}{3}$	$\pm\frac{-1+i-j-k}{2}$
$(\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{1}{\sqrt{3}}(-i+j-k)\sin\frac{2\pi}{3}$	$\pm\frac{-1-i+j-k}{2}$
$(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{1}{\sqrt{3}}(i+j+k)\sin\frac{2\pi}{3}$	$\pm\frac{-1+i+j+k}{2}$



Obr. 4.2: Ukážka osi rotácie spájajúcej vrchol a stred protiľahlej steny štvorstena.

Dokopy dostávame 12 kvaterniónových párov, ktoré popisujú rotácie z tetrahedrálnej grupy: ± 1, $\pm i$, $\pm j$, $\pm k$, $\pm\frac{1-i-j+k}{2}$, $\pm\frac{1+i-j-k}{2}$, $\pm\frac{1-i+j-k}{2}$, $\pm\frac{1+i+j+k}{2}$, $\pm\frac{-1-i-j+k}{2}$, $\pm\frac{-1+i-j-k}{2}$,$\pm\frac{-1-i+j-k}{2}$, $\pm\frac{-1+i+j+k}{2}$ a tvoria podgrupu $\mathbb{H}^1/\{\pm 1\}$.

Posledným krokom je, že danú podgrupu $\mathbb{H}^1/\{\pm 1\}$ pozdvihneme na podgrupu $\mathbb{H}^1$. To však prakticky znamená to, že pre každý kvaterniónový pár $\pm q$ musíme určiť, či jeho vzor bude q alebo $-q$, prípadne či sa v danej grupe vyskytnú obidva prvky. Keď si však vezmeme kvaterniónový pár $\pm j$, tak bez ohľadu na to, či ako vzor vyberieme j alebo $-j$, tak platí $j^2 = (-j)^2 = -1$, a teda v pôvodnej podgrupe $\mathbb{H}^1$ sa bude nachádzať vždy prvok -1, a teda automaticky pre každý kvaterniónový pár $\pm q$ tam získame q aj $-q$. Takto získame prvý typ konečnej podgrupy $\mathbb{H}^1$, známy aj ako binárna tetrahedrálna grupa.

Definícia 4.9 (binárna tetrahedrálna grupa)**.** Binárna tetrahedrálna grupa *je grupa* $2T = \{1, -1, i, -i, j, -j, k, -k, (\pm 1 \pm i \pm j \pm k)/2\}$ *rádu 24.*

Ešte si môžeme všimnúť súvislosť s rádmi z kapitoly 3, pretože podľa tvrdenia 3.15 je binárna tetrahedrálna grupa práve grupa jednotiek Hurwitzovho rádu.

4.3.2 Binárna oktahedrálna grupa

Ďalšia možnosť, ktorú preberieme je, že ako podgrupu $SO(3)$ budeme mať oktahedrálnu grupu O.

Definícia 4.10 (oktahedrálna grupa)**.** Oktahedrálna grupa O *je grupa rotačných symetrií pravidelného osemstena.*

Pri charakterizácií prvkov oktahedrálnej grupy vychádzame z knihy Polyhedra od P. R. Cromwella [7, Kapitola 8]. Nasledujúce tvrdenie by sa dalo dokázať obdobne ako pri tetrahedrálnej grupe. Najprv si uvedomíme, že rád oktahedrálnej grupy bude $8 \cdot 3 = 24$ a potom popíšeme týchto 24 rotačných symetrií. Následne sa vďaka ich typom dá nahliadnuť, že sú tieto popísané symetrie rôzne.

Tvrdenie 4.11 (prvky oktahedrálnej grupy)**.** *Rotačné symetrie pravidelného osemstena, a teda prvky oktahedrálnej grupy sú:*

- *identita,*
- *6 rotácií o uhol π okolo osi spájajúcej stredy dvoch protiľahlých hrán osemstena,*
- *4 rotácie o uhol $2\pi/3$ okolo osi spájajúcej stredy dvoch protiľahlých stien osemstena,*
- *4 rotácie o uhol $4\pi/3$ okolo osi spájajúcej stredy dvoch protiľahlých stien osemstena,*
- *3 rotácie o uhol $\pi/2$ okolo osi spájajúcej dva protiľahlé vrcholy osemstena,*
- *3 rotácie o uhol π okolo osi spájajúcej dva protiľahlé vrcholy osemstena,*
- *3 rotácie o uhol $3\pi/2$ okolo osi spájajúcej dva protiľahlé vrcholy osemstena.*

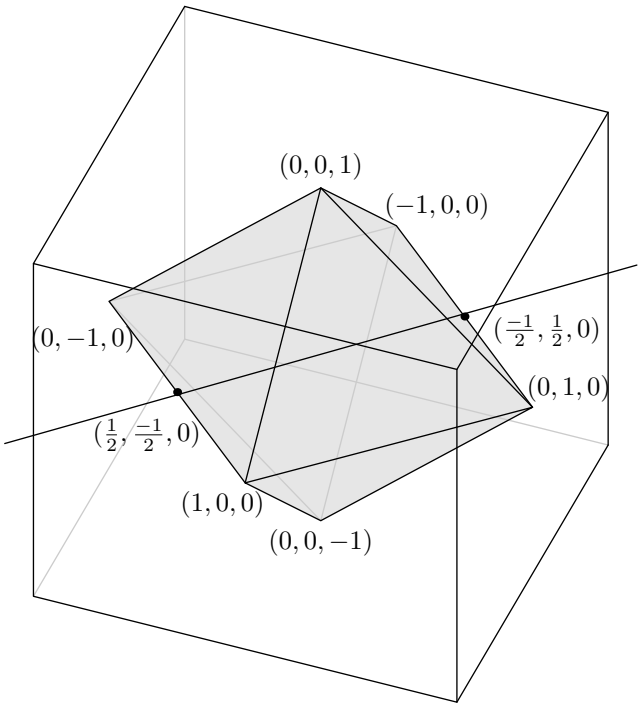
Prevedieme vlastné podrobné výpočty, ako v minulej sekcii, aby sme popísali prvky oktahedrálnej grupy ako kvaterniónové páry. Vezmeme si pravidelný osemsten, ktorý bude do kocky s hranou 2 vpísaný tak, že jeho vrcholy budú stredy stien kocky a ťažisko bude v bode (0,0,0). To znamená, že vrcholy pravidelného osemstena budú mať súradnice $(\pm1,0,0)$,$(0,\pm1,0)$ a $(0,0,\pm1)$, ako na obrázku 4.3.

Identita: Identickej rotácii vždy odpovedá kvaterniónový pár ±1.

Rotácia okolo osi spájajúcej stredy protiľahlých hrán osemstena o π:

Vďaka súradniciam vrcholov vieme vyrátať súradnice stredov jednotlivých hrán. Po dvojiciach protiľahlé stredy hrán sú $(\frac{\pm1}{2}, \frac{\pm1}{2},0)$, $(\frac{\mp1}{2}, \frac{\pm1}{2},0)$, $(\frac{\pm1}{2},0, \frac{\pm1}{2})$, $(\frac{\mp1}{2},0, \frac{\pm1}{2})$, $(0,\frac{\pm1}{2}, \frac{\pm1}{2})$ a $(0, \frac{\mp1}{2},\frac{\pm1}{2})$. Odtiaľ môžeme ako jednotkové vektory, ktoré určujú osi rotácií, zobrať $(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0)$, $(\frac{-1}{\sqrt{2}},\frac{1}{\sqrt{2}},0)$, $(\frac{1}{\sqrt{2}},0,\frac{1}{\sqrt{2}})$, $(\frac{-1}{\sqrt{2}},0,\frac{1}{\sqrt{2}})$, $(0,\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}})$ a $(0,\frac{-1}{\sqrt{2}},\frac{1}{\sqrt{2}})$. Tak ako v minulej podkapitole dorátame kvaterniónové páry.

Os rotácie	Uhol rotácie	Dosadenie	Kvaterniónový pár
$(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0)$	π	$\cos\frac{\pi}{2} + \frac{1}{\sqrt{2}}(i+j)\sin\frac{\pi}{2}$	$\pm\frac{1}{\sqrt{2}}(i+j)$
$(\frac{-1}{\sqrt{2}},\frac{1}{\sqrt{2}},0)$	π	$\cos\frac{\pi}{2} + \frac{1}{\sqrt{2}}(-i+j)\sin\frac{\pi}{2}$	$\pm\frac{1}{\sqrt{2}}(-i+j)$
$(\frac{1}{\sqrt{2}},0,\frac{1}{\sqrt{2}})$	π	$\cos\frac{\pi}{2} + \frac{1}{\sqrt{2}}(i+k)\sin\frac{\pi}{2}$	$\pm\frac{1}{\sqrt{2}}(i+k)$
$(\frac{-1}{\sqrt{2}},0,\frac{1}{\sqrt{2}})$	π	$\cos\frac{\pi}{2} + \frac{1}{\sqrt{2}}(-i+k)\sin\frac{\pi}{2}$	$\pm\frac{1}{\sqrt{2}}(-i+k)$
$(0,\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}})$	π	$\cos\frac{\pi}{2} + \frac{1}{\sqrt{2}}(j+k)\sin\frac{\pi}{2}$	$\pm\frac{1}{\sqrt{2}}(j+k)$
$(0,\frac{-1}{\sqrt{2}},\frac{1}{\sqrt{2}})$	π	$\cos\frac{\pi}{2} + \frac{1}{\sqrt{2}}(-j+k)\sin\frac{\pi}{2}$	$\pm\frac{1}{\sqrt{2}}(-j+k)$

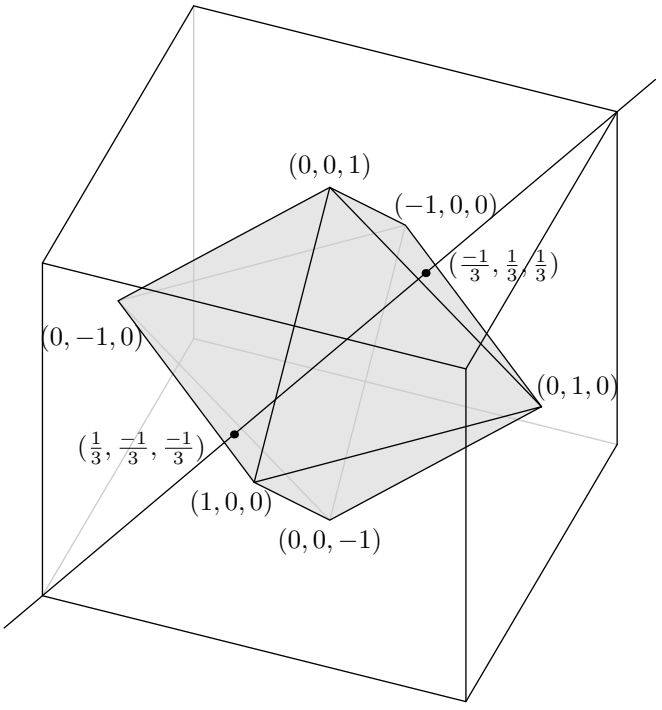


Obr. 4.3: Ukážka osi rotácie spájajúcej stredy protiľahlých hrán osemstena.

Rotácia okolo osi spájajúcej stredy protiľahlých stien osemstena o $2\pi/3$ alebo $4\pi/3$:

Podľa súradníc vrcholov osemstena vieme vyrátať súradnice stredov jeho stien. Konkrétne stredy príslušných protiľahlých stien sú $(\frac{-1}{3},\frac{-1}{3},\frac{1}{3})$ a $(\frac{1}{3},\frac{1}{3},\frac{-1}{3})$, $(\frac{1}{3},\frac{-1}{3},\frac{-1}{3})$ a $(\frac{-1}{3},\frac{1}{3},\frac{1}{3})$, $(\frac{-1}{3},\frac{1}{3},\frac{-1}{3})$ a $(\frac{1}{3},\frac{-1}{3},\frac{1}{3})$, $(\frac{1}{3},\frac{1}{3},\frac{1}{3})$ a $(\frac{-1}{3},\frac{-1}{3},\frac{-1}{3})$. Odtiaľ ľahko zrátame jednotkové vektory, ktoré definujú jednotlivé osi rotácií $(\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}})$, $(\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$, $(\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$ a $(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})$. Ostáva výpočet príslušných kvaterniónových párov.

Os rotácie	Uhol rotácie	Dosadenie	Kvaterniónový pár
$(\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{1}{\sqrt{3}}(-i-j+k)\sin\frac{\pi}{3}$	$\pm\frac{1-i-j+k}{2}$
$(\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{1}{\sqrt{3}}(i-j-k)\sin\frac{\pi}{3}$	$\pm\frac{1+i-j-k}{2}$
$(\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{1}{\sqrt{3}}(-i+j-k)\sin\frac{\pi}{3}$	$\pm\frac{1-i+j-k}{2}$
$(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{1}{\sqrt{3}}(i+j+k)\sin\frac{\pi}{3}$	$\pm\frac{1+i+j+k}{2}$
$(\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{1}{\sqrt{3}}(-i-j+k)\sin\frac{2\pi}{3}$	$\pm\frac{-1-i-j+k}{2}$
$(\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{1}{\sqrt{3}}(i-j-k)\sin\frac{2\pi}{3}$	$\pm\frac{-1+i-j-k}{2}$
$(\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{1}{\sqrt{3}}(-i+j-k)\sin\frac{2\pi}{3}$	$\pm\frac{-1-i+j-k}{2}$
$(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{1}{\sqrt{3}}(i+j+k)\sin\frac{2\pi}{3}$	$\pm\frac{-1+i+j+k}{2}$

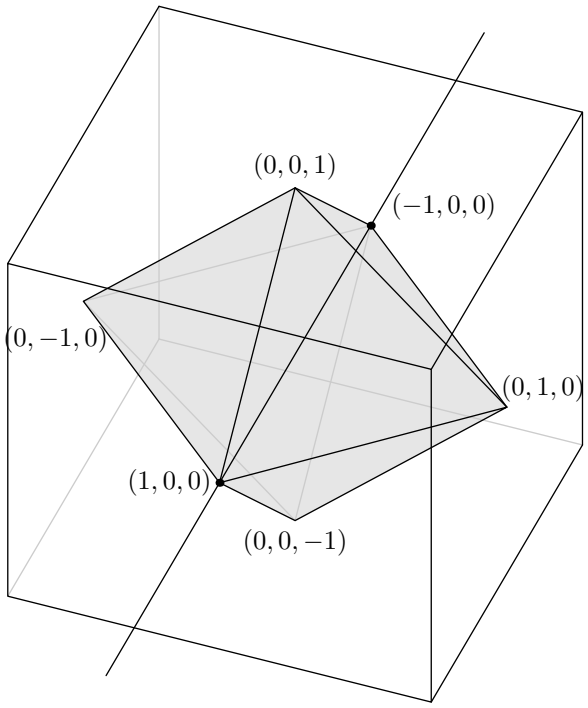


Obr. 4.4: Ukážka osi rotácie spájajúcej stredy protiľahlých stien osemstena.

Rotácia okolo osi spájajúcej dva protiľahlé vrcholy osemstena o $\pi/2$, π alebo $3\pi/2$:

Vzhľadom k tomu, že súradnice navzájom protiľahlých vrcholov osemstena sú po dvojiciach $(\pm 1,0,0)$, $(0,\pm 1,0)$ a $(0,0,\pm 1)$, tak osi rotácií, ktoré ich spájajú, sú určené napríklad jednotkovými vektormi (1,0,0), (0,1,0) a (0,0,1). To nám stačí na určenie jednotlivých kvaterniónových párov.

Os rotácie	Uhol rotácie	Dosadenie	Kvaterniónový pár
(1,0,0)	$\frac{\pi}{2}$	$\cos\frac{\pi}{4} + (1i + 0j + 0k)\sin\frac{\pi}{4}$	$\pm\frac{1}{\sqrt{2}}(1+i)$
(0,1,0)	$\frac{\pi}{2}$	$\cos\frac{\pi}{4} + (0i + 1j + 0k)\sin\frac{\pi}{4}$	$\pm\frac{1}{\sqrt{2}}(1+j)$
(0,0,1)	$\frac{\pi}{2}$	$\cos\frac{\pi}{4} + (0i + 0j + 1k)\sin\frac{\pi}{4}$	$\pm\frac{1}{\sqrt{2}}(1+k)$
(1,0,0)	π	$\cos\frac{\pi}{2} + (1i + 0j + 0k)\sin\frac{\pi}{2}$	$\pm i$
(0,1,0)	π	$\cos\frac{\pi}{2} + (0i + 1j + 0k)\sin\frac{\pi}{2}$	$\pm j$
(0,0,1)	π	$\cos\frac{\pi}{2} + (0i + 0j + 1k)\sin\frac{\pi}{2}$	$\pm k$
(1,0,0)	$\frac{3\pi}{2}$	$\cos\frac{3\pi}{4} + (1i + 0j + 0k)\sin\frac{3\pi}{4}$	$\pm\frac{1}{\sqrt{2}}(-1+i)$
(0,1,0)	$\frac{3\pi}{2}$	$\cos\frac{3\pi}{4} + (0i + 1j + 0k)\sin\frac{3\pi}{4}$	$\pm\frac{1}{\sqrt{2}}(-1+j)$
(0,0,1)	$\frac{3\pi}{2}$	$\cos\frac{3\pi}{4} + (0i + 0j + 1k)\sin\frac{3\pi}{4}$	$\pm\frac{1}{\sqrt{2}}(-1+k)$



Obr. 4.5: Ukážka osi rotácie spájajúcej dva protiľahlé vrcholy osemstena.

Prvky oktahedrálnej grupy nám popísalo 24 kvaterniónových párov, ktoré môžeme nájsť v predchádzajúcich tabuľkách. Rovnakou úvahou, ako pri tetrahedrálnej grupe, dostávame ďalšiu podgrupu $\mathbb{H}^1$, ktorá je známa aj ako binárna oktahedrálna grupa.

Definícia 4.12 (binárna oktahedrálna grupa)**.** Binárna oktahedrálna grupa *je* $2O = \{\pm 1, \pm i, \pm j, \pm k, \frac{\pm i \pm j}{\sqrt{2}}, \frac{\pm i \pm k}{\sqrt{2}}, \frac{\pm j \pm k}{\sqrt{2}}, \frac{\pm 1 \pm i}{\sqrt{2}}, \frac{\pm 1 \pm j}{\sqrt{2}}, \frac{\pm 1 \pm k}{\sqrt{2}}, \frac{\pm 1 \pm i \pm j \pm k}{2}\}$ *rádu 48.*

4.3.3 Binárna ikosahedrálna grupa

Treťou možnosťou je, že ako podgrupu $SO(3)$ máme ikosahedrálnu grupu. Popis jednotlivých prvkov tejto grupy môžeme opäť nájsť v knihe Polyhedra, P. R. Cromwell [7] a dôkaz by bol obdobný ako v predchádzajúcich častiach.

Definícia 4.13 (ikosahedrálna grupa)**.** *Ikosahedrálna grupa I je grupa rotačných symetrií pravidelného dvadsaťstenu.*

Tvrdenie 4.14 (prvky ikosahedrálnej grupy)**.** *Rotačné symetrie pravidelného dvadsaťstena, a teda prvky ikosahedrálnej grupy sú:*

- *identita,*
- *15 rotácií o uhol π okolo osi spájajúcej stredy dvoch protiľahlých hrán dvadsaťstena,*
- *10 rotácií o uhol $2\pi/3$ okolo osi spájajúcej stredy dvoch protiľahlých stien dvadsaťstena,*
- *10 rotácie o uhol $4\pi/3$ okolo osi spájajúcej stredy dvoch protiľahlých stien dvadsaťstena,*
- *6 rotácií o uhol $2\pi/5$ okolo osi spájajúcej dva protiľahlé vrcholy dvadsaťstena,*
- *6 rotácií o uhol $4\pi/5$ okolo osi spájajúcej dva protiľahlé vrcholy dvadsaťstena,*
- *6 rotácií o uhol $6\pi/5$ okolo osi spájajúcej dva protiľahlé vrcholy dvadsaťstena,*
- *6 rotácií o uhol $8\pi/5$ okolo osi spájajúcej dva protiľahlé vrcholy dvadsaťstena.*

Následne opäť zavedieme súradnice na popis vrcholov pravidelného dvadsaťstena. Môžeme ich nájsť napríklad v článku From the Icosahedron to E8, J. C. Baez [1]. Pre jednoduchosť, na popis súradníc zavedieme značenie pre takzvaný zlatý rez $\phi = (1 + \sqrt{5})/2$. Potom môžeme 12 vrcholov pravidelného dvadsaťstenu popísať súradnicami $(\pm 1, \pm\phi, 0)$, $(0, \pm 1, \pm\phi)$ a $(\pm\phi, 0, \pm 1)$.

Identita: Identickej rotácii vždy odpovedá kvaterniónový pár ± 1.

Rotácia okolo osi spájajúcej stredy protiľahlých hrán dvadsaťstena o π:

Pri rátaní stredov protiľahlých hrán dostávame napríklad dvojicu $(\frac{1}{2}, \frac{\phi+1}{2}, \frac{\phi}{2})$ a $(\frac{-1}{2}, \frac{-\phi-1}{2}, \frac{-\phi}{2})$, odkiaľ je os určená vektorom $(1, \phi+1, \phi)$. Rovnakým spôsobom dostaneme ešte $(\phi+1, \phi, 1)$, $(\phi, 1, \phi+1)$ a ku každému z nich ešte tri ďalšie vektory, ktoré majú vždy jednu zo súradníc zápornú. Plus ešte dostaneme trojicu vektorov $(\phi, 0, 0)$, $(0, \phi, 0)$ a $(0,0, \phi)$. Následne využívajúc vzťah $\sqrt{1^2 + \phi^2 + (1+\phi)^2} = 2\phi$ už dané vektory len vynormujeme. Dostaneme napríklad $\frac{1}{2\phi}(1, \phi+1, \phi) = (\frac{\phi^{-1}}{2}, \frac{\phi+1}{2\phi}, \frac{1}{2}) = (\frac{\phi^{-1}}{2}, \frac{\phi}{2}, \frac{1}{2})$.

Os rotácie	Uhol rot.	Dosadenie	Kvaterniónový pár
(1,0,0)	π	$\cos\frac{\pi}{2} + (1i + 0j + 0k)\sin\frac{\pi}{2}$	$\pm i$
(0,1,0)	π	$\cos\frac{\pi}{2} + (0i + 1j + 0k)\sin\frac{\pi}{2}$	$\pm j$
(0,0,1)	π	$\cos\frac{\pi}{2} + (0i + 0j + 1k)\sin\frac{\pi}{2}$	$\pm k$
$(\frac{\phi^{-1}}{2}, \frac{\phi}{2}, \frac{1}{2})$	π	$\cos\frac{\pi}{2} + \frac{1}{2}(\phi^{-1}i + \phi j + k)\sin\frac{\pi}{2}$	$\pm\frac{\phi^{-1}i+\phi j+k}{2}$
$(\frac{\phi}{2}, \frac{1}{2}, \frac{\phi^{-1}}{2})$	π	$\cos\frac{\pi}{2} + \frac{1}{2}(\phi i + j + \phi^{-1}k)\sin\frac{\pi}{2}$	$\pm\frac{\phi i+j+\phi^{-1}k}{2}$
$(\frac{1}{2}, \frac{\phi^{-1}}{2}, \frac{\phi}{2})$	π	$\cos\frac{\pi}{2} + \frac{1}{2}(i + \phi^{-1}j + \phi k)\sin\frac{\pi}{2}$	$\pm\frac{i+\phi^{-1}j+\phi k}{2}$
$(\frac{\phi^{-1}}{2}, \frac{\phi}{2}, \frac{-1}{2})$	π	$\cos\frac{\pi}{2} + \frac{1}{2}(\phi^{-1}i + \phi j - k)\sin\frac{\pi}{2}$	$\pm\frac{\phi^{-1}i+\phi j-k}{2}$
$(\frac{\phi}{2}, \frac{1}{2}, \frac{-\phi^{-1}}{2})$	π	$\cos\frac{\pi}{2} + \frac{1}{2}(\phi i + j - \phi^{-1}k)\sin\frac{\pi}{2}$	$\pm\frac{\phi i+j-\phi^{-1}k}{2}$
$(\frac{1}{2}, \frac{\phi^{-1}}{2}, \frac{-\phi}{2})$	π	$\cos\frac{\pi}{2} + \frac{1}{2}(i + \phi^{-1}j - \phi k)\sin\frac{\pi}{2}$	$\pm\frac{i+\phi^{-1}j-\phi k}{2}$
$(\frac{\phi^{-1}}{2}, \frac{-\phi}{2}, \frac{1}{2})$	π	$\cos\frac{\pi}{2} + \frac{1}{2}(\phi^{-1}i - \phi j + k)\sin\frac{\pi}{2}$	$\pm\frac{\phi^{-1}i-\phi j+k}{2}$
$(\frac{\phi}{2}, \frac{-1}{2}, \frac{\phi^{-1}}{2})$	π	$\cos\frac{\pi}{2} + \frac{1}{2}(\phi i - j + \phi^{-1}k)\sin\frac{\pi}{2}$	$\pm\frac{\phi i-j+\phi^{-1}k}{2}$
$(\frac{1}{2}, \frac{-\phi^{-1}}{2}, \frac{\phi}{2})$	π	$\cos\frac{\pi}{2} + \frac{1}{2}(i - \phi^{-1}j + \phi k)\sin\frac{\pi}{2}$	$\pm\frac{i-\phi^{-1}j+\phi k}{2}$
$(\frac{-\phi^{-1}}{2}, \frac{\phi}{2}, \frac{1}{2})$	π	$\cos\frac{\pi}{2} + \frac{1}{2}(-\phi^{-1}i + \phi j + k)\sin\frac{\pi}{2}$	$\pm\frac{-\phi^{-1}i+\phi j+k}{2}$
$(\frac{-\phi}{2}, \frac{1}{2}, \frac{\phi^{-1}}{2})$	π	$\cos\frac{\pi}{2} + \frac{1}{2}(-\phi i + j + \phi^{-1}k)\sin\frac{\pi}{2}$	$\pm\frac{-\phi i+j+\phi^{-1}k}{2}$
$(\frac{-1}{2}, \frac{\phi^{-1}}{2}, \frac{\phi}{2})$	π	$\cos\frac{\pi}{2} + \frac{1}{2}(-i + \phi^{-1}j + \phi k)\sin\frac{\pi}{2}$	$\pm\frac{-i+\phi^{-1}j+\phi k}{2}$

Rotácia okolo osi spájajúcej stredy protiľahlých stien dvadsaťstena o $2\pi/3$ alebo $4\pi/3$:

Podľa súradníc vieme určiť stredy protiľahlých stien a z toho následne vektory, ktoré určujú osi rotácií. Dostaneme $(\frac{2(\phi+1)}{3}, \frac{2(\phi+1)}{3}, \frac{2(\phi+1)}{3})$ a ešte ďalšie tri podobné vektory, kde je ale stále jedna súradnica záporná, ďalej $(0, \frac{2(2\phi+1)}{3}, \frac{2\phi}{3})$, $(0, \frac{2(2\phi+1)}{3}, \frac{-2\phi}{3})$ a k obom ďalšie dva vektory, ktoré vznikli cyklickou zámenou ich súradníc. Z prvého typu vektorov po vynormovaní dostaneme $\frac{1}{\sqrt{3}}(1,1,1)$ a ďalšie tri s jednou zápornou súradnicou. Z druhého typu získame $\frac{2}{3\sqrt{3}+\sqrt{15}}(0,2\phi+1,\phi)$, $\frac{2}{3\sqrt{3}+\sqrt{15}}(0,2\phi+1,-\phi)$ plus cyklické zámeny. V druhom prípade sme vychádzali zo vzťahu pre normu vektoru so zložkami $0, \phi, 2\phi+1$, a teda $\sqrt{\phi^2+(2\phi+1)^2} = \frac{3\sqrt{3}+\sqrt{15}}{2}$. Dokopy sme získali 10 jednotkových vektorov, ktoré určujú osi rotácií. Každý z nich spojíme s uhlom rotácie $2\pi/3$ aj $4\pi/3$ a dorátame odpovedajúce kvaterniónové páry.

Os rotácie	Uh. r.	Dosadenie	Kvat. pár
$(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{1}{\sqrt{3}}(i+j+k)\sin\frac{\pi}{3}$	$\pm\frac{1+i+j+k}{2}$
$(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{1}{\sqrt{3}}(i+j-k)\sin\frac{\pi}{3}$	$\pm\frac{1+i+j-k}{2}$
$(\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{1}{\sqrt{3}}(i-j+k)\sin\frac{\pi}{3}$	$\pm\frac{1+i-j+k}{2}$
$(\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{1}{\sqrt{3}}(-i+j+k)\sin\frac{\pi}{3}$	$\pm\frac{1-i+j+k}{2}$
$\frac{2}{3\sqrt{3}+\sqrt{15}}(0,2\phi+1,\phi)$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{2}{3\sqrt{3}+\sqrt{15}}((2\phi+1)j+\phi k)\sin\frac{\pi}{3}$	$\pm\frac{1+\phi j+\phi^{-1}k}{2}$
$\frac{2}{3\sqrt{3}+\sqrt{15}}(0,2\phi+1,-\phi)$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{2}{3\sqrt{3}+\sqrt{15}}((2\phi+1)j-\phi k)\sin\frac{\pi}{3}$	$\pm\frac{1+\phi j-\phi^{-1}k}{2}$
$\frac{2}{3\sqrt{3}+\sqrt{15}}(2\phi+1,\phi,0)$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{2}{3\sqrt{3}+\sqrt{15}}((2\phi+1)i+\phi j)\sin\frac{\pi}{3}$	$\pm\frac{1+\phi i+\phi^{-1}j}{2}$
$\frac{2}{3\sqrt{3}+\sqrt{15}}(2\phi+1,-\phi,0)$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{2}{3\sqrt{3}+\sqrt{15}}((2\phi+1)i-\phi j)\sin\frac{\pi}{3}$	$\pm\frac{1+\phi i-\phi^{-1}j}{2}$
$\frac{2}{3\sqrt{3}+\sqrt{15}}(\phi,0,2\phi+1)$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{2}{3\sqrt{3}+\sqrt{15}}(\phi i+(2\phi+1)k)\sin\frac{\pi}{3}$	$\pm\frac{1+\phi^{-1}i+\phi k}{2}$
$\frac{2}{3\sqrt{3}+\sqrt{15}}(-\phi,0,2\phi+1)$	$\frac{2\pi}{3}$	$\cos\frac{\pi}{3}+\frac{2}{3\sqrt{3}+\sqrt{15}}(-\phi i+(2\phi+1)k)\sin\frac{\pi}{3}$	$\pm\frac{1-\phi^{-1}i+\phi k}{2}$
$(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{1}{\sqrt{3}}(i+j+k)\sin\frac{2\pi}{3}$	$\pm\frac{-1+i+j+k}{2}$
$(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}})$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{1}{\sqrt{3}}(i+j-k)\sin\frac{2\pi}{3}$	$\pm\frac{-1+i+j-k}{2}$
$(\frac{1}{\sqrt{3}},\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{1}{\sqrt{3}}(i-j+k)\sin\frac{2\pi}{3}$	$\pm\frac{-1+i-j+k}{2}$
$(\frac{-1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{1}{\sqrt{3}}(-i+j+k)\sin\frac{2\pi}{3}$	$\pm\frac{-1-i+j+k}{2}$
$\frac{2}{3\sqrt{3}+\sqrt{15}}(0,2\phi+1,\phi)$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{2}{3\sqrt{3}+\sqrt{15}}((2\phi+1)j+\phi k)\sin\frac{2\pi}{3}$	$\pm\frac{-1+\phi j+\phi^{-1}k}{2}$
$\frac{2}{3\sqrt{3}+\sqrt{15}}(0,2\phi+1,-\phi)$	$\frac{2\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{2}{3\sqrt{3}+\sqrt{15}}((2\phi+1)j-\phi k)\sin\frac{2\pi}{3}$	$\pm\frac{-1+\phi j-\phi^{-1}k}{2}$
$\frac{2}{3\sqrt{3}+\sqrt{15}}(2\phi+1,\phi,0)$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{2}{3\sqrt{3}+\sqrt{15}}((2\phi+1)i+\phi j)\sin\frac{2\pi}{3}$	$\pm\frac{-1+\phi i+\phi^{-1}j}{2}$
$\frac{2}{3\sqrt{3}+\sqrt{15}}(2\phi+1,-\phi,0)$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{2}{3\sqrt{3}+\sqrt{15}}((2\phi+1)i-\phi j)\sin\frac{2\pi}{3}$	$\pm\frac{-1+\phi i-\phi^{-1}j}{2}$
$\frac{2}{3\sqrt{3}+\sqrt{15}}(\phi,0,2\phi+1)$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{2}{3\sqrt{3}+\sqrt{15}}(\phi i+(2\phi+1)k)\sin\frac{2\pi}{3}$	$\pm\frac{-1+\phi^{-1}i+\phi k}{2}$
$\frac{2}{3\sqrt{3}+\sqrt{15}}(-\phi,0,2\phi+1)$	$\frac{4\pi}{3}$	$\cos\frac{2\pi}{3}+\frac{2}{3\sqrt{3}+\sqrt{15}}(-\phi i+(2\phi+1)k)\sin\frac{2\pi}{3}$	$\pm\frac{-1-\phi^{-1}i+\phi k}{2}$

Rotácia okolo osi spájajúcej dva protiľahlé vrcholy dvadsaťstena o $2\pi/5$**,** $4\pi/5$**,** $6\pi/5$ **alebo** $8\pi/5$**:**

Keďže poznáme súradnice vrcholov, tak vieme vyrátať šesť vektorov, ktoré určujú osi rotácií: $(0,2,2\phi)$, $(0,-2,2\phi)$ a pre každý ešte zvyšné cyklické zámeny. Využívajúc vzťah $\sqrt{1^2+\phi^2}=\frac{\sqrt{5+\sqrt{5}}}{\sqrt{2}}$ dostávame vynormované jednotkové vektory, ktoré určujú osi rotácií: $\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(0,1,\phi)$, $\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(0,-1,\phi)$ a ich cyklické zámeny.

Os rotácie	Uhol rot.	Dosadenie	Kvat. pár
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(0,1,\phi)$	$\frac{2\pi}{5}$	$\cos\frac{\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(j+\phi k)\sin\frac{\pi}{5}$	$\pm\frac{\phi+\phi^{-1}j+k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(0,-1,\phi)$	$\frac{2\pi}{5}$	$\cos\frac{\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(-j+\phi k)\sin\frac{\pi}{5}$	$\pm\frac{\phi-\phi^{-1}j+k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi,0,1)$	$\frac{2\pi}{5}$	$\cos\frac{\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi i+k)\sin\frac{\pi}{5}$	$\pm\frac{\phi+i+\phi^{-1}k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi,0,-1)$	$\frac{2\pi}{5}$	$\cos\frac{\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi i-k)\sin\frac{\pi}{5}$	$\pm\frac{\phi+i-\phi^{-1}k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(1,\phi,0)$	$\frac{2\pi}{5}$	$\cos\frac{\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(i+\phi j)\sin\frac{\pi}{5}$	$\pm\frac{\phi+\phi^{-1}i+j}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(-1,\phi,0)$	$\frac{2\pi}{5}$	$\cos\frac{\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(-i+\phi j)\sin\frac{\pi}{5}$	$\pm\frac{\phi-\phi^{-1}i+j}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(0,1,\phi)$	$\frac{4\pi}{5}$	$\cos\frac{2\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(j+\phi k)\sin\frac{2\pi}{5}$	$\pm\frac{\phi^{-1}+j+\phi k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(0,-1,\phi)$	$\frac{4\pi}{5}$	$\cos\frac{2\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(-j+\phi k)\sin\frac{2\pi}{5}$	$\pm\frac{\phi^{-1}-j+\phi k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi,0,1)$	$\frac{4\pi}{5}$	$\cos\frac{2\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi i+k)\sin\frac{2\pi}{5}$	$\pm\frac{\phi^{-1}+\phi i+k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi,0,-1)$	$\frac{4\pi}{5}$	$\cos\frac{2\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi i-k)\sin\frac{2\pi}{5}$	$\pm\frac{\phi^{-1}+\phi i-k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(1,\phi,0)$	$\frac{4\pi}{5}$	$\cos\frac{2\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(i+\phi j)\sin\frac{2\pi}{5}$	$\pm\frac{\phi^{-1}+i+\phi j}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(-1,\phi,0)$	$\frac{4\pi}{5}$	$\cos\frac{2\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(-i+\phi j)\sin\frac{2\pi}{5}$	$\pm\frac{\phi^{-1}-i+\phi j}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(0,1,\phi)$	$\frac{6\pi}{5}$	$\cos\frac{3\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(j+\phi k)\sin\frac{3\pi}{5}$	$\pm\frac{-\phi^{-1}+j+\phi k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(0,-1,\phi)$	$\frac{6\pi}{5}$	$\cos\frac{3\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(-j+\phi k)\sin\frac{3\pi}{5}$	$\pm\frac{-\phi^{-1}-j+\phi k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi,0,1)$	$\frac{6\pi}{5}$	$\cos\frac{3\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi i+k)\sin\frac{3\pi}{5}$	$\pm\frac{-\phi^{-1}+\phi i+k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi,0,-1)$	$\frac{6\pi}{5}$	$\cos\frac{3\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi i-k)\sin\frac{3\pi}{5}$	$\pm\frac{-\phi^{-1}+\phi i-k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(1,\phi,0)$	$\frac{6\pi}{5}$	$\cos\frac{3\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(i+\phi j)\sin\frac{3\pi}{5}$	$\pm\frac{-\phi^{-1}+i+\phi j}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(-1,\phi,0)$	$\frac{6\pi}{5}$	$\cos\frac{3\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(-i+\phi j)\sin\frac{3\pi}{5}$	$\pm\frac{-\phi^{-1}-i+\phi j}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(0,1,\phi)$	$\frac{8\pi}{5}$	$\cos\frac{4\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(j+\phi k)\sin\frac{4\pi}{5}$	$\pm\frac{-\phi+\phi^{-1}j+k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(0,-1,\phi)$	$\frac{8\pi}{5}$	$\cos\frac{4\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(-j+\phi k)\sin\frac{4\pi}{5}$	$\pm\frac{-\phi-\phi^{-1}j+k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi,0,1)$	$\frac{8\pi}{5}$	$\cos\frac{4\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi i+k)\sin\frac{4\pi}{5}$	$\pm\frac{-\phi+i+\phi^{-1}k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi,0,-1)$	$\frac{8\pi}{5}$	$\cos\frac{4\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(\phi i-k)\sin\frac{4\pi}{5}$	$\pm\frac{-\phi+i-\phi^{-1}k}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(1,\phi,0)$	$\frac{8\pi}{5}$	$\cos\frac{4\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(i+\phi j)\sin\frac{4\pi}{5}$	$\pm\frac{-\phi+\phi^{-1}i+j}{2}$
$\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(-1,\phi,0)$	$\frac{8\pi}{5}$	$\cos\frac{4\pi}{5}+\frac{\sqrt{2}}{\sqrt{5+\sqrt{5}}}(-i+\phi j)\sin\frac{4\pi}{5}$	$\pm\frac{-\phi-\phi^{-1}i+j}{2}$

Na predchádzajúcich stranách sme v niekoľkých tabuľkách popísali 60 kvaterniónových párov, ktoré vzhľadom k násobeniu tvoria podgrupu $\mathbb{H}^1/\{\pm 1\}$. Opäť rozlíšením prvkov v každom páre získavame ďalší typ podgrupy $\mathbb{H}^1$, známy ako binárna ikosahedrálna grupa.

Definícia 4.15 (binárna ikosahedrálna grupa)**.** Binárna ikosahedrálna grupa *je* $2I = \{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}, \frac{\pm 1 \pm \phi i \pm \phi^{-1} j}{2}, \frac{\pm 1 \pm \phi j \pm \phi^{-1} k}{2}, \frac{\pm 1 \pm \phi^{-1} i \pm \phi k}{2}, \frac{\pm \phi \pm i \pm \phi^{-1} k}{2}, \frac{\pm \phi \pm \phi^{-1} j \pm k}{2}, \frac{\pm \phi \pm \phi^{-1} i \pm j}{2}, \frac{\pm \phi^{-1} \pm \phi i \pm k}{2}, \frac{\pm \phi^{-1} \pm j \pm \phi k}{2}, \frac{\pm \phi^{-1} \pm i \pm \phi j}{2}, \frac{\pm \phi^{-1} i \pm \phi j \pm k}{2}, \frac{\pm \phi i \pm j \pm \phi^{-1} k}{2}, \frac{\pm i \pm \phi^{-1} j \pm \phi k}{2}\}$ *rádu 120.*

4.3.4 Binárna dihedrálna grupa

Predposlednou možnosťou je, že ako podgrupu $SO(3)$ dostaneme dihedrálnu grupu D_n rádu $2n$. Pri jednotlivých vlastnostiach dihedrálnych grúp budeme vychádzať z textu Dihedral groups, K. Conrad [3].

Definícia 4.16 (dihedrálna grupa)**.** Dihedrálna grupa D_n *rádu* $2n$ *je grupa symetrií (rotácií a reflexií) pravidelného* n*-uholníka.*

Tvrdenie 4.17 (prvky dihedrálnej grupy)**.** *Symetrie pravidelného* n*-uholníka, a teda prvky dihedrálnej grupy* D_n *sú:*

- n *rotácií o uhol* $k\frac{2\pi}{n}$ *pre* $k = 0, 1, \ldots n-1$ *okolo osi, ktorá je kolmá na rovinu, v ktorej* n*-uholník leží a prechádza cez ťažisko* n*-uholníka,*
- n *reflexií (alebo aj rotácií o uhol* π*):*
  - *ak je* n *nepárne, tak okolo osí spájajúcich vrchol so stredom protiľahlej strany* n*-uholníka,*
  - *ak je* n *párne, tak okolo osí spájajúcich buď dva protiľahlé vrcholy alebo dva stredy protiľahlých strán* n*-uholníka.*

Dôkaz. To, že zobrazenia popísané v znení vety sú všetko symetrie pravidelného n-uholníka, sa dá ľahko nahliadnuť. Druhou úlohou je ukázať, že symetrií môže byť najviac $2n$, a teda, že sme ich popísali všetky. Vyberme si v n-uholníku dva susedné vrcholy. Ak určíme, kde sa zobrazia tieto dva vrcholy, tak už tým bude určené celé zobrazenie. Prvý vrchol sa môže zobraziť na ľubovoľný vrchol n-uholníka, a teda na n rôznych pozícií. K nemu susedný vrchol má na výber dva susedné vrcholy okolo obrazu prvého vrcholu. Dokopy teda najviac $n \cdot 2 = 2n$ rôznych možností.

□

Namiesto toho, aby sme pomocou kvaterniónov popísali všetkých $2n$ prvkov dihedrálnej grupy D_n, sa tentokrát pozrieme iba na generátory tejto grupy. Môžeme si uvedomiť, že na vygenerovanie celej grupy nám stačia dva prvky: jeden rádu n a jeden rádu 2. Je to tak vďaka tomu, že každú rotáciu o uhol $k\frac{2\pi}{n}$ pre $k = 0, 1, \ldots n-1$ vieme vygenerovať zložením k rotácií o uhol $2\pi/n$. V prípade reflexií vieme postupovať obdobne. Každú z n reflexií vieme vygenerovať zložením jednej ľubovoľne vybranej reflexie a následne niekoľkých rotácií o uhol $2\pi/n$.

Tvrdenie 4.18 (generátory dihedrálnej grupy)**.** *Všetky prvky dihedrálnej grupy D_n vieme vygenerovať pomocou dvoch prvkov:*

- *rotácie o uhol $2\pi/n$ okolo osi, ktorá je kolmá na rovinu, v ktorej n-uholník leží a prechádza cez ťažisko n-uholníka,*
- *rotácie o uhol π (resp. reflexie) okolo osi prechádzajúcej cez dva protiľahlé vrcholy n-uholníka (ak je n párne) alebo osi prechádzajúcej cez vrchol a stred protiľahlej strany n-uholníka (ak je n nepárne).*

Opäť si zavedieme súradnice. Predpokladajme, že celý pravidelný n-uholník leží v rovine, ktorá je daná rovnicou $x = 0$. Ďalej predpokladajme, že ťažisko nášho n-uholníka je bod (0,0,0) a je natočený tak, že jeden z jeho vrcholov leží na y-ovej osi v bode (0,1,0). Tým je poloha n-uholníka presne určená.

Rotácia okolo osi, ktorá je kolmá na rovinu, v ktorej n-uholník leží a prechádza cez ťažisko n-uholníka o $2\pi/n$:

Keďže ťažisko n-uholníka je v bode (0,0,0) a celý n-uholník leží v rovine $x = 0$, tak os tejto rotácie je vlastne x-ová súradnicová os, a teda ju vieme popísať napríklad jednotkovým vektorom (1,0,0).

Potom danú rotáciu vieme obdobne, ako v predchádzajúcich kapitolách, popísať jednotkovým kvaterniónovým párom $\pm q = \pm(\cos\frac{2\pi}{2n} + (1i + 0j + 0k)\sin\frac{2\pi}{2n}) = \pm(\cos\frac{\pi}{n} + i\sin\frac{\pi}{n})$ v závislosti na n.

Rotácia okolo osi prechádzajúcej cez dva protiľahlé vrcholy n-uholníka (ak je n párne) alebo osi prechádzajúcej cez vrchol a stred protiľahlej strany n-uholníka (ak je n nepárne) o uhol π:

Môžeme si vybrať akúkoľvek os reflexie pravidelného n-uholníka. Súradnice sme si navrhli tak, že jeden vrchol n-uholníka je vždy v bode (0,1,0). Vezmeme si teda os reflexie, ktorá prechádza týmto vrcholom. Bez ohľadu na to, či je n párne alebo nepárne, tak os reflexie, ktorá prechádza vrcholom (0,1,0) bude určite prechádzať aj ťažiskom daného n-uholníka. To znamená, že túto os vieme popísať jednotkovým vektorom (0,1,0).

Potom je táto rotácia o uhol π popísaná jednotkovým kvaterniónovým párom $\pm q = \pm(\cos\frac{\pi}{2} + (0i + 1j + 0k)\sin\frac{\pi}{2}) = \pm j$.

Dokopy sme vďaka popisu generátorov dostali, že pre dihedrálnu grupu D_n rádu $2n$ platí $D_n = \langle \pm j, \pm(\cos\frac{\pi}{n} + i\sin\frac{\pi}{n})\rangle$. Z toho znova rovnakou úvahou dostávame ďalší typ podgrupy $\mathbb{H}^1$, a to

$$Dic_n = \langle j, -j, \cos\frac{\pi}{n} + i\sin\frac{\pi}{n}, -(\cos\frac{\pi}{n} + i\sin\frac{\pi}{n})\rangle.$$

Keďže, ale platí vzťah $j^2 = -1$, tak nám v zápise ako generátory stačia prvky j, $\cos\frac{\pi}{n} + i\sin\frac{\pi}{n}$ a dostávame binárnu dihedrálnu grupu.

Definícia 4.19 (binárna dihedrálna grupa)**.** Binárna dihedrálna grupa *(resp. dicyklická grupa) je pre $n > 1$ grupa $Dic_n = \langle j, \cos\frac{\pi}{n} + i\sin\frac{\pi}{n}\rangle$ rádu $4n$.*

4.3.5 Cyklická grupa

Posledným prípadom je, že ako podgrupu $SO(3)$ máme cyklickú grupu C_n rádu n. To znamená, že daná grupa je generovaná jedným prvkom rádu n. Keď sa na tento generátor pozrieme ako na prvok $SO(3)$, tak sa jedná o rotáciu v $\mathbb{R}^3$, ktorú vieme popísať osou rotácie určenou jednotkovým vektorom (x,y,z) a uhlom $\theta \in [0, 2\pi]$. Keďže má mať daný prvok rád n, tak to znamená, že n zložení tejto rotácie nám dá identitu. Z toho môžeme usúdiť, že sa jedná o rotáciu o uhol $\theta = \frac{a \cdot 2\pi}{n}$ pre nejaké $a \in \mathbb{N}, a < n$. Podobne, ako v predchádzajúcich sekciách, vieme tento prvok potom popísať ako kvaterniónový pár $\pm(\cos\frac{a\pi}{n} + (xi+yj+zk)\sin\frac{a\pi}{n})$.

Dostali sme $C_n = \langle \pm(\cos\frac{a\pi}{n} + (xi+yj+zk)\sin\frac{a\pi}{n})\rangle$ ako podgrupu $\mathbb{H}^1/\{\pm 1\}$. Následne chceme získať príslušnú podgrupu $\mathbb{H}^1$, ktorá môže byť vzorom C_n pri homomorfizme $\mathbb{H}^1$ a $\mathbb{H}^1/\{\pm 1\}$. Najprv sa pozrieme na potenciálny vzor generátora $\pm(\cos\frac{a\pi}{n} + (xi+yj+zk)\sin\frac{a\pi}{n})$. Ten jednoduchší prípad je, že by išlo o grupy $\langle -(\cos\frac{a\pi}{n} + (xi+yj+zk)\sin\frac{a\pi}{n})\rangle$ alebo $\langle \cos\frac{a\pi}{n} + (xi+yj+zk)\sin\frac{a\pi}{n}\rangle$. V oboch prípadoch to bude cyklická grupa.

Poslednou možnosťou je, že by vzorom bola grupa $\langle \cos\frac{a\pi}{n} + (xi+yj+zk)\sin\frac{a\pi}{n}, -(\cos\frac{a\pi}{n} + (xi+yj+zk)\sin\frac{a\pi}{n})\rangle$. V takomto prípade dokážeme, že opäť ide o cyklickú grupu. Označme a' a n' také prirodzené čísla, že $NSD(a',n') = 1$ a zároveň $a/n = a'/n'$. Potom môžu nastať dve možnosti:

- Platí, že a' je nepárne. Potom máme $(\cos\frac{a'\pi}{n'} + (xi+yj+zk)\sin\frac{a'\pi}{n'})^{n'} = \cos\frac{n'a'\pi}{n'} + (xi+yj+zk)\sin\frac{n'a'\pi}{n'} = \cos(a'\pi) + (xi+yj+zk)\sin(a'\pi) = \cos(a'\pi) = -1$. Prvá úprava sa dá dokázať indukciou. V poslednom kroku využívame to, že $a'\pi$ je nepárny násobok π, a teda kosínus nadobúda hodnotu -1. To znamená, že prvok $\cos\frac{a'\pi}{n'} + (xi+yj+zk)\sin\frac{a'\pi}{n'}$ dokáže vygenerovať -1, a teda aj druhý z generátorov, čiže je to cyklická grupa.

- Platí, že a' je párne. Potom n' je nepárne, keďže $NSD(a',n') = 1$. V takom prípade dostávame $(-(\cos\frac{a'\pi}{n'} + (xi+yj+zk)\sin\frac{a'\pi}{n'}))^{n'} = (-1)^{n'}(\cos\frac{n'a'\pi}{n'} + (xi+yj+zk)\sin\frac{n'a'\pi}{n'}) = (-1)^{n'}(\cos(a'\pi) + (xi+yj+zk)\sin(a'\pi)) = (-1)^{n'}\cos(a'\pi) = -1$. Posledná úprava platí vďaka tomu, že $a'\pi$ je párnym násobkom π, a teda $\cos(a'\pi) = 1$, zatiaľ čo $(-1)^{n'} = -1$, keďže n' je nepárne. Opäť z toho ale dostávame, že ako generátor stačí prvok $-(\cos\frac{a'\pi}{n'} + (xi+yj+zk)\sin\frac{a'\pi}{n'})$ a ide o cyklickú grupu.

Týmto sme prešli všetky prípustné konečné podgrupy v $\mathbb{H}^1/\{\pm 1\}$ a z nich odvodili možné konečné podgrupy $\mathbb{H}^1$. Tieto závery zhrnieme v nasledujúcej vete.

Veta 4.20 (konečné podgrupy $\mathbb{H}^1$)**.** *Každá konečná podgrupa $\mathbb{H}^1$ je jedného z nasledujúcich typov:*

- *$2T$: binárna tetrahedrálna grupa rádu 24,*
- *$2O$: binárna oktahedrálna grupa rádu 48,*
- *$2I$: binárna ikosahedrálna grupa rádu 120,*
- *Dic_n: binárna dihedrálna grupa (dicyklická) rádu $4n$,*
- *C_n: cyklická grupa rádu n.*

Na pripomenutie len povedzme, že charakterizácia z poslednej vety 4.20 je priamo charakterizáciou aj konečných podgrúp $\mathbb{H}^\times$, ako sme v úvode tejto kapitoly dokázali.

4.4 Prezentácie konečných podgrúp $\mathbb{H}^\times$

V tejto podkapitole si uvedieme prezentácie jednotlivých grúp, s ktorými sme vyššie pracovali. Vo všeobecnosti grupa G má prezentáciu $\langle S|R\rangle$, kde S znamená množinu generátorov danej grupy a R množinu vzťahov, ktoré platia medzi danými generátormi. Úplne formálne môžeme povedať, že G má prezentáciu $\langle S|R\rangle$, ak je grupa G izomorfná faktorgrupe voľnej grupy generovanej S podľa normálnej podgrupy generovanej vzťahmi R.

Napríklad, keď sa povie cyklická grupa rádu n, tak vieme, že to značí grupu, ktorá má jeden generátor, ktorý je rádu n. Tento fakt by sa dal pomocou prezentácie grúp zapísať ako $C_n \simeq \langle r \mid r^n = 1\rangle$.

V nasledujúcich tabuľkách si zhrnieme najprv prezentácie všetkých konečných podgrúp $SO(3)$ (respektíve $\mathbb{H}^1/\{\pm 1\}$) a následne aj z nich odvodených konečných podgrúp $\mathbb{H}^1$ (respektíve $\mathbb{H}^\times$). Jednotlivé prezentácie sa dajú nájsť buď priamo v knihe Quaternion algebras, J. Voight [11], z ktorej sme vychádzali, alebo v knihe Generators and Relations for Discrete Groups, Harold S. M. Coxeter a William O. J. Moser [6].

Konečná podgrupa $SO(3)$	Rád	Prezentácia grupy
Cyklická	n	$C_n \simeq \langle r \mid r^n = 1\rangle$
Dihedrálna	$2n$	$D_n \simeq \langle r, s \mid r^n = s^2 = (sr)^2 = 1\rangle$
Tetrahedrálna	12	$T \simeq \langle r, s, t \mid r^2 = s^3 = t^3 = rst = 1\rangle$
Oktahedrálna	24	$O \simeq \langle r, s, t \mid r^2 = s^3 = t^4 = rst = 1\rangle$
Ikosahedrálna	60	$I \simeq \langle r, s, t \mid r^2 = s^3 = t^5 = rst = 1\rangle$

Samozrejme, nejde o jediný spôsob, ako vyjadriť prezentáciu daných grúp. Napríklad, pri posledných troch grupách by sme mohli z podmienky $rst = 1$ vyjadriť t ako $t = s^{-1}r^{-1} = (rs)^{-1}$. Čo by následne z podmienky $t^a = 1$, kde $a = 3,\ 4,\ 5$ spravilo podmienku $((rs)^{-1})^a = 1$, čiže po úprave $(rs)^a = 1$. Takže napríklad tetrahedrálnu grupu by sme mohli prezentovať ako $T \simeq \langle r, s \mid r^2 = s^3 = (rs)^3 = 1\rangle$.

Prezentácia dihedrálnej grupy vychádza priamo z popisu generátorov, ktoré sme uviedli v tvrdení 4.18. Dôkazy prezentácií zvyšných troch grúp nebudeme uvádzať všetky. Pre predstavu ukážeme aspoň dôkaz izomorfizmu pri prezentácii tetrahedrálnej grupy, pričom pri ostatných by sa dalo postupovať obdobným spôsobom.

Pri dôkaze nám bude vyhovovať práve upravená prezentácia, a teda dokážeme, že $T \simeq \langle r, s \mid r^2 = s^3 = (rs)^3 = 1\rangle$. Majme zobrazenie $\phi : \langle r, s\rangle \to T$, pričom $\langle r, s\rangle$ znamená voľnú grupu generovanú r, s. Toto zobrazenie definujeme pomocou obrazov generátorov, čiže tým, že $r \to \pm i$ a $s \to \pm(-1 + i + j + k)/2$. Dané zobrazenie je homomorfizmus.

Ako prvú vec ukážeme, že je dané zobrazenie na. Na to postačí, ak ukážeme, že vieme vygenerovať každý prvok grupy T, pričom budeme vychádzať z popisu danej grupy pomocou kvaterniónových párov. To znamená $T = \{\pm 1, \pm i, \pm j, \pm k, \pm\frac{1-i-j+k}{2}, \pm\frac{1+i-j-k}{2}, \pm\frac{1-i+j-k}{2}, \pm\frac{1+i+j+k}{2}, \pm\frac{-1-i-j+k}{2}, \pm\frac{-1+i-j-k}{2}, \pm\frac{-1-i+j-k}{2}, \pm\frac{-1+i+j+k}{2}\}$, ako sme ukázali v jednej z predchádzajúcich sekcií v definícii 4.9. Pri výpočtoch budeme brať $r = i$ a $s = (-1 + i + j + k)/2$ a následne z výsledku spravíme kvaterniónový pár. Všetky tieto prvky vieme vygenerovať nasledujúcim spôsobom:

- $r = i \longrightarrow \pm i$,
- $s = \frac{-1+i+j+k}{2} \longrightarrow \pm\frac{-1+i+j+k}{2}$,
- $r^2 = i^2 = -1 \longrightarrow \pm 1$,
- $rs = i(\frac{-1+i+j+k}{2}) = \frac{-1-i-j+k}{2} \longrightarrow \pm\frac{-1-i-j+k}{2}$,
- $s^2 = (\frac{-1+i+j+k}{2})^2 = \frac{-1-i-j-k}{2} \longrightarrow \pm\frac{1+i+j+k}{2}$,
- $sr = (\frac{-1+i+j+k}{2})i = \frac{-1-i+j-k}{2} \longrightarrow \pm\frac{-1-i+j-k}{2}$,
- $rsr = isr = i(\frac{-1-i+j-k}{2}) = \frac{1-i+j+k}{2} \longrightarrow \pm\frac{-1+i-j-k}{2}$,
- $rs^2 = i(\frac{-1-i-j-k}{2}) = \frac{1-i+j-k}{2} \longrightarrow \pm\frac{1-i+j-k}{2}$,
- $srs = (\frac{-1+i+j+k}{2})rs = (\frac{-1+i+j+k}{2})(\frac{-1-i-j+k}{2}) = \frac{1+i-j-k}{2} \longrightarrow \pm\frac{1+i-j-k}{2}$,
- $s^2r = (\frac{-1-i-j-k}{2})i = \frac{1-i-j+k}{2} \longrightarrow \pm\frac{1-i-j+k}{2}$,
- $srs^2 = (sr)(s^2) = (\frac{-1-i+j-k}{2})(\frac{-1-i-j-k}{2}) = k \longrightarrow \pm k$,
- $s^2rs = (s^2)(rs) = (\frac{-1-i-j-k}{2})(\frac{-1-i-j+k}{2}) = j \longrightarrow \pm j$.

Zobrazenie ϕ je grupový homomorfizmus, takže podľa 1. vety o izomorfizme platí $\langle r, s\rangle/\mathrm{Ker}\ \phi \simeq \mathrm{Im}\ \phi$. Zároveň sme ukázali, že je dané zobrazenie na, a teda $\mathrm{Im}\ \phi = T$. Dokopy máme $\langle r, s\rangle/\mathrm{Ker}\ \phi \simeq T$. Ostáva nám ukázať, že $\mathrm{Ker}\ \phi = \langle r^2, s^3, (rs)^3\rangle$. Ak by sa nám to podarilo, tak potom by platilo:

$$\langle r, s \mid r^2 = s^3 = (rs)^3 = 1\rangle \simeq \langle r, s\rangle/\langle r^2, s^3, (rs)^3\rangle \simeq T.$$

Vieme ukázať, že platí:

- $r^2 = i^2 = -1 \longrightarrow \pm 1$,
- $s^3 = s^2s = (\frac{-1-i-j-k}{2})(\frac{-1+i+j+k}{2}) = 1 \longrightarrow \pm 1$,
- $(rs)^3 = (rsr)(srs) = (\frac{1-i+j+k}{2})(\frac{1+i-j-k}{2}) = 1 \longrightarrow \pm 1$.

Odtiaľ dostávame, že Ker $\phi \supseteq \langle r^2, s^3, (rs)^3 \rangle$. Ostáva overiť, že v Ker ϕ nie je nejaký ďalší prvok. My však už vieme, že platí $\langle r, s \rangle / \text{Ker } \phi \simeq T$, a že T má rád 12, čo znamená, že aj $\langle r, s \rangle / \text{Ker } \phi$ musí mať rád 12. Ukážeme, že ak by sa Ker $\phi = \langle r^2, s^3, (rs)^3 \rangle$, tak potom má $\langle r, s \rangle / \text{Ker } \phi$ práve 12 prvkov. To vylučuje, že by bol v Ker ϕ nejaký ďalší prvok, pretože potom by $\langle r, s \rangle / \text{Ker } \phi$ malo menej prvkov, ako musí mať.

Budeme postupne tvoriť slová rôznych dĺžok z generátorov r, s. Vieme, že sa v nich nemôžu vyskytovať dve r respektíve tri s za sebou, pretože potom je táto časť rovná 1. Zároveň vieme, že 12 prvkov, ktoré sme využili pri dôkaze toho, že je ϕ na, sú rôzne.

- dĺžky 1: r, s, 1
- dĺžky 2: rs, sr, ss
- dĺžky 3: rsr, rss, srs, ssr

Vždy, keď budujeme slová dĺžky k, vychádzame zo slov dĺžky $k-1$, ktoré boli rôzne a pridávame ako posledný znak r a s tak, aby slová neobsahovali za sebou dve r ani tri s. Zároveň, keďže $r^2 = 1$, tak $r = r^{-1}$, rovnako $s^3 = 1$ implikuje $s^2 = s^{-1}$, a posledná podmienka $(rs)^3 = 1$ sa dá interpretovať aj ako $rsrs = s^{-1}r^{-1}$. Tieto pravidlá budeme používať.

- dĺžky 4:
  - $rsrs = s^{-1}r^{-1} = s^2r$ - tento prvok už máme
  - $rssr = r(s^2)(r) = r(s^{-1}r^{-1}) = r(rsrs) = (rr)srs = srs$ - tento prvok už máme
  - $srsr = r^{-1}s^{-1} = rs^2$ - tento prvok už máme
  - $srss$ - nový prvok
  - $ssrs$ - nový prvok
- dĺžky 5:
  - $srssr = s(rssr) = ssrs$ - tento prvok už máme
  - $ssrsr = s(srsr) = srss$ - tento prvok už máme
  - $ssrss = ss(r)(ss) = ss(r^{-1}s^{-1}) = ss(srsr) = (sss)rsr = rsr$ - tento prvok už máme

Postupne sme generovali všetky možné prvky $\langle r, s \mid r^2 = s^3 = (rs)^3 = 1 \rangle$ a našli sme práve 12 rôznych. Všetky ostatné vieme pomocou prepisovacích pravidiel previesť na jeden z týchto prvkov. Týmto sme dokázali správnosť prezentácie tetrahedrálnej grupy.

Ako sme už avizovali, pre úplnosť na záver ešte uvedieme prezentácie jednotlivých konečných podgrúp $\mathbb{H}^\times$.

Konečná podgrupa $\mathbb{H}^\times$	Rád	Prezentácia grupy
Cyklická	n	$C_n \simeq \langle r \mid r^n = 1 \rangle$
Binárna dihedrálna	$4n$	$Dic_n \simeq \langle r, s \mid r^{2n} = 1, s^2 = r^n, s^{-1}rs = r^{-1} \rangle$
Binárna tetrahedrálna	24	$2T \simeq \langle r, s, t, u \mid r^2 = s^3 = t^3 = rst = u, u^2 = 1 \rangle$
Binárna oktahedrálna	48	$2O \simeq \langle r, s, t, u \mid r^2 = s^3 = t^4 = rst = u, u^2 = 1 \rangle$
Binárna ikosahedrálna	120	$2I \simeq \langle r, s, t, u \mid r^2 = s^3 = t^5 = rst = u, u^2 = 1 \rangle$

5. Grupy jednotiek v rádoch v hamiltonovských kvaterniónoch

V tejto kapitole sa dostávame k ďalšej kľúčovej časti tejto práce, ktorú sme už viackrát spomínali, a to klasifikácii konečných grúp jednotiek v rádoch v hamiltonovských kvaterniónoch. Danú tému podrobne rozoberieme a vychádzať budeme z knihy Quaternion algebras od J.Voighta [11, Kapitola 11].

Na začiatok predpokladajme, že máme kvaterniónovú algebru $B = \left(\frac{a,b}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ takú, že platí $\left(\frac{a,b}{\mathbb{R}}\right) \simeq \mathbb{H}$. To podľa vety 2.11 vieme, že nastane práve vtedy, ak $a < 0$ a zároveň $b < 0$. Následne v danej kvaterniónovej algebre vezmeme rád $\mathcal{O} \subseteq B$. Naším cieľom bude skúmať jeho grupu jednotiek, a teda $\mathcal{O}^\times$.

Spomínali sme, že budeme skúmať grupy jednotiek v rádoch v hamiltonovských kvaterniónoch. Toto označenie vyplýva z voľby kvaterniónovej algebry, a teda z toho, že platí:

$$\mathcal{O}^\times \subseteq \mathcal{O} \subseteq B = \left(\frac{a,b}{\mathbb{Q}}\right) \subseteq \left(\frac{a,b}{\mathbb{R}}\right) \simeq \mathbb{H}.$$

Tvrdenie 5.1. *Platí $\mathcal{O}^\times \subseteq \mathcal{O}^1 = \{\alpha \in \mathcal{O} \mid N(\alpha) = 1\}$ a grupa $\mathcal{O}^\times$ je konečná.*

Dôkaz. V prvom rade si uvedomíme, že keď $\alpha \in \mathcal{O}^\times$, $\alpha = t + xi + yj + zk$, tak potom podľa definície 1.12 platí $N(\alpha) = t^2 - ax^2 - by^2 + abz^2$. V našom prípade ale vieme, že pre kvaterniónovú algebru, v ktorej sa nachádzame, platí $a, b < 0$, a teda môžeme písať $N(\alpha) = t^2 + |a|x^2 + |b|y^2 + |ab|z^2$. Z čoho priamo vidíme, že norma je vždy nezáporné racionálne číslo, a teda konkrétne $N(\mathcal{O}^\times) \subseteq \mathbb{Q}_{\geq 0}$.

Keďže $\mathcal{O}$ je $\mathbb{Z}$-rád, tak spojením tvrdení 3.7 a 3.8 dostávame, že každý prvok rádu $\mathcal{O}$ má celočíselnú stopu aj normu, a teda $N(\mathcal{O}^\times) \subseteq \mathbb{Z}_{\geq 0}$. Na záver si ešte všimneme, že keď $\alpha \in \mathcal{O}^\times$, tak existuje $\beta \in \mathcal{O}$ taká, že $\alpha\beta = 1$ a odtiaľ aplikovaním normy získame $N(\alpha)N(\beta) = 1$. Z toho vyplýva, že norma prvku z $\mathcal{O}^\times$ má vždy inverz, keďže $N(\alpha), N(\beta) \in \mathbb{Z}$, a teda $N(\mathcal{O}^\times) \subseteq \mathbb{Z}_{\geq 0}^\times = \{1\}$. Z čoho priamo plynie $\mathcal{O}^\times \subseteq \mathcal{O}^1$.

Na to, aby sme ukázali, že $\mathcal{O}^\times$ je konečná grupa, tak ukážeme, že $\mathcal{O}^1$ je konečná. Keďže $\mathcal{O}^1 \subseteq \mathbb{H}$, tak na prvky $\mathcal{O}^1$ sa môžeme pozerať ako na body na elipsoide v $\mathbb{R}^4$. Keďže $\mathcal{O}$ je $\mathbb{Z}$-rád, a teda $\mathbb{Z}$-mriežka, tak sa na prvky $\mathcal{O}^1$ môžeme pozerať ako na mrežové body na elipsoide v $\mathbb{R}^4$. Tých je konečne mnoho, a teda $\mathcal{O}^1$ je konečná množina.

□

Spojením tvrdenia 5.1 s predchádzajúcou úvahou dostávame, že $\mathcal{O}^\times$ je konečná podgrupa $\mathbb{H}$. Keďže $\mathcal{O}^\times$ je grupa jednotiek a neobsahuje 0, tak dokonca platí $\mathcal{O}^\times$ je konečná podgrupa $\mathbb{H}^\times$. V tejto chvíli presne vidíme význam toho, prečo sme sa v minulej kapitole venovali úplnej klasifikácii konečných podgrúp $\mathbb{H}^\times$. Našim cieľom teraz bude vrátiť sa k vete 4.20, ktorá charakterizuje aj konečné podgrupy $\mathbb{H}^\times$, a prejdením jednotlivých možností charakterizovať $\mathcal{O}^\times$.

5.1 Kvadratické polia

Pred tým, ako prejdeme ku charakterizácií grúp jednotiek, zhrnieme si časť teórie ohľadom kvadratických polí, ktorú budeme pri charakterizácii potrebovať. Pôjde hlavne o teóriu týkajúcu sa celistvých prvkov. Pri nasledujúcich dôkazoch budeme vychádzať predovšetkým z článku Factoring in quadratic fields, K. Conrad [4].

Definícia 5.2 (kvadratické pole)**.** *Nech $d \in \mathbb{Z}$, $d \neq 1$ a platí, že d nie je deliteľné žiadnou druhou mocninou celého čísla okrem 1 (inak povedané d je bezštvorcové). Potom $\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x,y \in \mathbb{Q}\}$ je* kvadratické pole.

Kvadratické polia $\mathbb{Q}(\sqrt{d})$ rozdeľujeme podľa toho, či je d kladné alebo záporné, na reálne a imaginárne kvadratické polia.

Definícia 5.3 (reálne, imaginárne kvadratické pole)**.** *Nech $d \in \mathbb{Z}$, $d \neq 1$ a d je bezštvorcové. Potom kvadratické pole $\mathbb{Q}(\sqrt{d})$ je* reálne*, ak platí $d > 0$ a* imaginárne*, ak platí $d < 0$.*

Definícia 5.4 (celistvý prvok, okruh celistvých prvkov)**.** *Nech $\mathbb{Q}(\sqrt{d})$ je kvadratické pole. Potom prvok $\gamma \in \mathbb{Q}(\sqrt{d})$ je* celistvý*, ak je koreňom monického polynómu s koeficientami zo $\mathbb{Z}$. Všetky prvky $\mathbb{Q}(\sqrt{d})$, ktoré sú celistvé, tvoria* okruh celistvých prvkov*, ktorý značíme $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.*

Pre kvadratické polia môžeme opäť obdobne zaviesť pojem združeného prvku, normy a stopy. Následne vďaka tomu môžeme charakterizovať, ktoré prvky ležia v okruhu celistvých prvkov.

Definícia 5.5 (združený prvok)**.** *Nech $\mathbb{Q}(\sqrt{d})$ je kvadratické pole a $\gamma \in \mathbb{Q}(\sqrt{d})$, $\gamma = x + y\sqrt{d}$. Potom definujeme k nemu* združený prvok *ako $\overline{\gamma} = x - y\sqrt{d}$.*

Definícia 5.6 (norma, stopa v kvadratickom poli)**.** *Nech $\mathbb{Q}(\sqrt{d})$ je kvadratické pole a $\gamma \in \mathbb{Q}(\sqrt{d})$, $\gamma = x + y\sqrt{d}$. Potom definujeme* normu γ *ako $n(\gamma) = \gamma\overline{\gamma} = x^2 - dy^2$ a stopu ako $tr(\gamma) = \gamma + \overline{\gamma} = 2x$.*

Opäť sa dá ľahko overiť, že aj v kvadratickom poli $\mathbb{Q}(\sqrt{d})$ je stopa aditívna a norma multiplikatívna. Pre každý prvok $\gamma \in \mathbb{Q}(\sqrt{d})$ platí, že je koreňom monického polynómu tvaru $(x-\gamma)(x-\overline{\gamma}) = x^2 - (\gamma+\overline{\gamma})x + \gamma\overline{\gamma} = x^2 - tr(\gamma)x + n(\gamma)$.

Tvrdenie 5.7. *Nech $\mathbb{Q}(\sqrt{d})$ je kvadratické pole a $\gamma \in \mathbb{Q}(\sqrt{d})$. Označme minimálny monický polynóm pre γ ako $m_\gamma(x) \in \mathbb{Q}[x]$. Potom platí, že $\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ práve vtedy, keď $m_\gamma(x) \in \mathbb{Z}[x]$.*

Dôkaz. Keď $m_\gamma(x) \in \mathbb{Z}[x]$, tak zjavne z definície rovno $\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Potrebujeme teda dokázať opačnú implikáciu. Predpokladajme, že γ je celistvý prvok. To znamená, že existuje monický polynóm $f(x) \in \mathbb{Z}[x]$ taký, že $f(\gamma) = 0$. Potom v $\mathbb{Q}[x]$ platí, že $m_\gamma(x)$ delí polynóm $f(x)$. Tým pádom vieme, že existuje $g(x) \in \mathbb{Q}[x]$ taký, že $m_\gamma(x)g(x) = f(x)$. Z toho rovno vidíme, že $g(x)$ bude tiež monický polynóm.

Chceme ukázať, že $m_\gamma(x) \in \mathbb{Z}[x]$. Pre spor predpokladajme, že to neplatí. Potom existuje prvočíslo p také, že delí aspoň jeden menovateľ koeficientu v $m_\gamma(x)$. Označme $u > 0$ najmenšie prirodzené číslo také, že žiaden z koeficientov polynómu $p^u m_\gamma(x)$ už nemá menovateľ deliteľný p. Rovnako označme $v \geq 0$ najmenšie prirodzené číslo také, že to isté platí o $p^v g(x)$. Pôvodnú rovnosť môžeme upraviť na $p^u m_\gamma(x) p^v g(x) = p^{(u+v)} f(x)$.

Keďže ľavá strana rovnosti už nemá žiaden menovateľ deliteľný p, tak sa na danú rovnosť môžeme pozrieť modulo p. Na pravej strane dostávame 0 v $\mathbb{Z}_p[x]$, zatiaľ čo na ľavej strane máme súčin dvoch nenulových polynómov $p^u m_\gamma(x)$ a $p^v g(x)$. Vieme, že sú nenulové v $\mathbb{Z}_p[x]$, keďže vzhľadom na minimalitu u a v v nich existuje koeficient, ktorý nie je deliteľný p. V $\mathbb{Z}_p[x]$ ale nie je možné, aby dva nenulové prvky dali nulový súčin, a teda máme spor.

□

Tvrdenie 5.8. *Nech $\mathbb{Q}(\sqrt{d})$ je kvadratické pole a $\gamma \in \mathbb{Q}(\sqrt{d})$. Potom platí, že $\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ práve vtedy, keď $n(\gamma), tr(\gamma) \in \mathbb{Z}$.*

Dôkaz. Nech $n(\gamma), tr(\gamma) \in \mathbb{Z}$. Potom spomínaný polynóm $x^2 - tr(\gamma)x + n(\gamma)$ je monický, γ je jeho koreňom a má koeficienty zo $\mathbb{Z}$. Z toho plynie, že γ je celistvý prvok.

Pre opačnú implikáciu predpokladajme, že $\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Jediné celistvé prvky z $\mathbb{Q}$ sú priamo prvky $\mathbb{Z}$, a teda ak $\gamma \in \mathbb{Q}$, tak platí $\gamma \in \mathbb{Z}$ a priamo z definície aj $n(\gamma), tr(\gamma) \in \mathbb{Z}$. Predpokladajme teda, že $\gamma \notin \mathbb{Q}$. Potom minimálny polynóm pre γ má stupeň práve 2. Vyššie zmienený polynóm $x^2 - tr(\gamma)x + n(\gamma)$ má stupeň 2 a γ je jeho koreňom, čiže je to minimálny monický polynóm pre γ. Potom z predchádzajúceho tvrdenia 5.7 vieme, že $n(\gamma), tr(\gamma) \in \mathbb{Z}$.

□

Tvrdenie 5.9. *Nech $\mathbb{Q}(\sqrt{d})$ je kvadratické pole. Potom platí, že $(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})^\times = \{\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \mid n(\gamma) = \pm 1\}$.*

Dôkaz. Nech $\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Predpokladajme, že je γ jednotkou. Potom existuje $\delta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ taká, že platí $\gamma\delta = 1$. Po aplikovaní normy na obe strany dostávame rovnosť $n(\gamma)n(\delta) = n(1) = 1$. Podľa predchádzajúceho tvrdenia 5.8 vieme, že $n(\gamma) \in \mathbb{Z}$, a teda jediné možnosti sú, že $n(\gamma) = \pm 1$.

Pre opačnú implikáciu predpokladajme, že $n(\gamma) = \pm 1$. Vieme, že prvky γ a $\overline{\gamma}$ majú rovnakú normu a stopu. Takže keď $\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, tak potom aj $\overline{\gamma} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ podľa tvrdenia 5.8. Potom z definície normy máme $\pm 1 = n(\gamma) = \gamma\overline{\gamma}$, čiže $\pm\overline{\gamma}$ je inverzný prvok k γ.

□

Teraz už máme dostatok informácií, aby sme exaktne popísali, ako vyzerá okruh celistvých prvkov kvadratického poľa a následne popísali grupu jednotiek v okruhu celistvých prvkov aspoň pre prípad imaginárneho kvadratického poľa. Nasledujúce tvrdenia sa dajú nájsť napríklad v knihe A Classical Introduction to Modern Number Theory, K. Ireland a M. Rosen [8, Kapitola 13].

Veta 5.10 (okruh celistvých prvkov kvadratického poľa)**.** *Nech $d \in \mathbb{Z}$, $d \neq 1$, d je bezštvorcové a $\mathbb{Q}(\sqrt{d})$ je kvadratické pole. Potom platí:*

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{ak } d \equiv 2,3 \mod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{ak } d \equiv 1 \mod 4. \end{cases}$$

Dôkaz. Najprv ukážeme jednu inklúziu. Nech $\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, $\gamma = x + y\sqrt{d}$, kde x, $y \in \mathbb{Q}$. Podľa tvrdenia 5.8 platí, že ak γ je celistvý prvok, tak $tr(\gamma) = 2x \in \mathbb{Z}$ a aj $n(\gamma) = x^2 - dy^2 \in \mathbb{Z}$. Keďže $2x$, $x^2 - dy^2 \in \mathbb{Z}$, tak aj $(2x)^2$, $4(x^2 - dy^2) \in \mathbb{Z}$, čo nás vedie k tomu, že aj $(2x)^2 - 4(x^2 - dy^2) = 4dy^2 = (2y)^2 d \in \mathbb{Z}$. Vzhľadom na to, že $d \in \mathbb{Z}$ je bezštvorcové, tak vlastne dostávame $2y \in \mathbb{Z}$.

To znamená, že môžeme zaviesť značenie $m = 2x$, $n = 2y$, kde m, $n \in \mathbb{Z}$. Zároveň podmienka $x^2 - y^2 d \in \mathbb{Z}$ vedie k tomu, že $m^2/4 - dn^2/4 \in \mathbb{Z}$, a teda $m^2 - dn^2 \equiv 0 \mod 4$. Vieme, že modulo 4 máme kvadratické zvyšky iba 0 alebo 1. Teraz rozoberieme dve možnosti:

- Nech $d \equiv 2,3 \mod 4$. Potom platí $0 \equiv m^2 - dn^2 \equiv m^2 + 2n^2$ alebo $m^2 + n^2 \mod 4$. V oboch prípadoch je kvôli kvadratickým zvyškom jediné možné riešenie, keď $m^2 \equiv n^2 \equiv 0 \mod 4$. To nastane práve vtedy, keď m aj n sú párne čísla, a teda x, $y \in \mathbb{Z}$. Ukázali sme, že v tomto prípade $\gamma \in \mathbb{Z}[\sqrt{d}]$.
- Nech $d \equiv 1 \mod 4$. Potom $0 \equiv m^2 - dn^2 \equiv m^2 - n^2 \mod 4$. Odtiaľ plynie, že $m^2 \equiv n^2 \mod 4$, a teda m a n musia mať rovnakú paritu. Platí, že:

  $$\gamma = x + y\sqrt{d} = \frac{m + n\sqrt{d}}{2} = \frac{m+n}{2} + n\frac{-1+\sqrt{d}}{2}.$$

  Keďže m a n majú rovnakú paritu, tak vieme, že $(m+n)/2 \in \mathbb{Z}$. Čo znamená, že $\gamma \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Teraz ukážeme opačnú inklúziu. Najprv predpokladajme, že $\gamma \in \mathbb{Z}[\sqrt{d}]$, čiže $\gamma = x + y\sqrt{d}$, kde x, $y \in \mathbb{Z}$. Potom priamo z definície $tr(\gamma) = 2x \in \mathbb{Z}$ a aj $n(\gamma) = x^2 - dy^2 \in \mathbb{Z}$. Takže podľa tvrdenia 5.8 je γ celistvý prvok.

Teraz nech platí $\gamma \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, čiže $\gamma = x + y(\frac{1+\sqrt{d}}{2})$, kde x, $y \in \mathbb{Z}$. Potom vieme vykonať úpravu $\gamma = x + y(\frac{1+\sqrt{d}}{2}) = (x + y/2) + (y/2)\sqrt{d}$. Odtiaľ opäť vieme vyjadriť stopu $tr(\gamma) = 2(x + y/2) = 2x + y$ a normu $n(\gamma) = (x + y/2)^2 - d(y/2)^2 = x^2 + xy + y^2(1-d)/4$. Rovno vidíme, že stopa je celočíselná, a keďže v tomto prípade je $d \equiv 1 \mod 4$, tak aj norma je celočíselná. Rovnakou úvahou dostávame, že γ je celistvá.

□

Veta 5.11 (grupa jednotiek v okruhu celistvých prvkov imaginárneho kvadratického poľa)**.** *Nech $d \in \mathbb{Z}$, $d \neq 1$, d je bezštvorcové a $\mathbb{Q}(\sqrt{d})$ je imaginárne kvadratické pole. Potom platí:*

- *ak $d = -1$, tak potom grupa jednotiek $(\mathcal{O}_{\mathbb{Q}(\sqrt{-1})})^\times = \{1, i, -1, -i\}$,*
- *ak $d = -3$, tak potom grupa jednotiek $(\mathcal{O}_{\mathbb{Q}(\sqrt{-3})})^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$, kde $\omega = (-1 + \sqrt{-3})/2$,*
- *ak $d = -2$ alebo $d < -3$, tak potom grupa jednotiek $(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})^\times = \{1, -1\}$.*

Dôkaz. Nech $\gamma \in (\mathcal{O}_{\mathbb{Q}(\sqrt{d})})^\times$, potom podľa tvrdenia 5.9 platí, že $n(\gamma) = \pm 1$. Najprv predpokladajme, že $d \equiv 2, 3 \mod 4$. Potom podľa vety 5.10 vieme, že $\gamma = x + y\sqrt{d}$ pre $x, y \in \mathbb{Z}$. Z definície normy máme $n(\gamma) = n(x+y\sqrt{d}) = x^2+|d|y^2$. Spojením týchto podmienok dostávame $x^2 + |d|y^2 = 1$. Potom môžu nastať dve možnosti:

- Platí, že $d = -1$. Potom máme rovnosť $x^2 + y^2 = 1$, a teda jediné riešenia sú $x = \pm 1$, $y = 0$ alebo $x = 0$, $y = \pm 1$. Z toho plynie, že $\gamma \in \{1, i, -1, -i\}$.
- Platí, že $d \neq -1$. Potom nutne $y = 0$ a jediné riešenia rovnice $x^2+|d|y^2 = 1$ sú $x = \pm 1$, čiže $\gamma \in \{1, -1\}$.

Teraz predpokladajme, že $d \equiv 1 \mod 4$. Potom z vety 5.10 môžeme odvodiť, že platí $\gamma = (x + y\sqrt{d})/2$ pre $x, y \in \mathbb{Z}$, $x \equiv y \mod 2$. Z definície normy opäť dostávame $n(\gamma) = n((x+y\sqrt{d})/2)) = (x/2)^2+|d|(y/2)^2$. Spojením s podmienkou $n(\gamma) = \pm 1$ dostávame jedinú možnosť, ktorá môže nastať $(x/2)^2 + |d|(y/2)^2 = 1$, čo je po úprave $x^2 + |d|y^2 = 4$. Potom sú znova dve možnosti:

- Platí, že $d = -3$. Máme rovnosť $x^2 + 3y^2 = 4$, kde $x, y \in \mathbb{Z}$, $x \equiv y \mod 2$. Jediné riešenia sú $x = \pm 1$, $y = \pm 1$ alebo $x = \pm 2$, $y = 0$. Po dosadení vidíme, že to znamená, že $\gamma \in \{\pm 1, (\pm 1 \pm \sqrt{-3})/2\} = \{\pm 1, \pm\omega, \pm\omega^2\}$.
- Platí, že $d \neq -3$. Potom jediné riešenie $x^2 + |d|y^2 = 4$ je $x = \pm 2$, $y = \pm 0$, čiže $\gamma \in \{1, -1\}$.

Týmto rozborom sme pokryli všetky možnosti a ukázali, že $(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})^\times$ je nutne jedným z troch spomínaných typov.

□

5.2 Cyklická grupa ako grupa jednotiek

Teraz môžeme prejsť k jednotlivým prípadom, ktoré sme avizovali na konci úvodu piatej kapitoly. Prvá možnosť, ktorú máme je, že $\mathcal{O}^\times$ bude cyklická grupa. To znamená, že existuje prvok α, ktorý celé $\mathcal{O}^\times$ generuje, a teda platí $\mathcal{O}^\times = \langle\alpha\rangle$. Keďže $\alpha \in \mathcal{O}$ a $\mathcal{O}$ je $\mathbb{Z}$-rád, tak podľa tvrdení 3.7 a 3.8 platí, že $N(\alpha), Tr(\alpha) \in \mathbb{Z}$. Rovno na úvod môžeme predpokladať, že $\alpha \neq \pm 1$. Inak dostávame rovno triviálnu cyklickú grupu $\mathcal{O}^\times = \{1\}$ alebo $\mathcal{O}^\times = \{\pm 1\}$ cyklickú grupu rádu 2.

Lemma 5.12. *Nech $\left(\frac{a,b}{F}\right)$ je kvaterniónová algebra. Potom pre prvok $\alpha \in \left(\frac{a,b}{F}\right)$ platí, že spĺňa rovnicu $\alpha^2 - Tr(\alpha)\alpha + N(\alpha) = 0$.*

Dôkaz. Podľa definícií 1.12 a 1.13 vieme, že $N(\alpha) = \alpha\overline{\alpha}$ a $Tr(\alpha) = \alpha + \overline{\alpha}$. Potom môžeme písať:

$$\alpha^2 - Tr(\alpha)\alpha + N(\alpha) = \alpha^2 - (\alpha + \overline{\alpha})\alpha + \alpha\overline{\alpha} = \alpha^2 - \alpha^2 - \overline{\alpha}\alpha + \alpha\overline{\alpha} = -\overline{\alpha}\alpha + \alpha\overline{\alpha}$$

Na to, aby platila rovnosť zo znenia lemmy, potrebujeme ešte ukázať, že platí vzťah $\overline{\alpha}\alpha = \alpha\overline{\alpha}$. Nech $\alpha = t + xi + yj + zk$, $\alpha \in \left(\frac{a,b}{F}\right)$ a vyjadríme oba súčiny:

- $\alpha\overline{\alpha} = (t+xi+yj+zk)(t-xi-yj-zk) = t^2-txi-tyj-tzk+txi-ax^2-xyk-xzaj+tyj+xyk-by^2+yzbi+tzk+xzaj-yzbi+abz^2 = t^2-ax^2-by^2+abz^2$
- $\overline{\alpha}\alpha = (t-xi-yj-zk)(t+xi+yj+zk) = t^2+txi+tyj+tzk-txi-ax^2-xyk-xzaj-tyj+xyk-by^2+yzbi-tzk+xzaj-yzbi+abz^2 = t^2-ax^2-by^2+abz^2$

Z toho už rovno platí, že $\alpha^2 - Tr(\alpha)\alpha + N(\alpha) = 0$.

□

Vďaka poslednej lemme vieme, že konkrétne aj náš generátor α grupy $\mathcal{O}^\times$ spĺňa rovnicu $\alpha^2 - Tr(\alpha)\alpha + N(\alpha) = 0$. Spolu s faktom $N(\alpha), Tr(\alpha) \in \mathbb{Z}$, dostávame, že generátor α spĺňa kvadratickú rovnicu s celočíselnými koeficientami. Keďže ale $\alpha \in \mathcal{O}^\times$ a ukázali sme, že $\mathcal{O}^\times \subseteq \mathcal{O}^1$, tak rovno vieme, že $N(\alpha) = 1$. Tým pádom si môžeme danú rovnicu upraviť na $x^2 - Tr(\alpha)x + 1 = 0$. Keď sa na túto rovnicu pozeráme nad $\mathbb{H}$, tak môže mať samozrejme veľa koreňov, ktoré nevieme presne vyjadriť. Avšak, ak sa na danú rovnicu pozrieme nad $\mathbb{C}$, tak ako kvadratická rovnica má aj komplexné riešenie, ktoré označíme β a vieme ho vyjadriť podľa klasického vzorca pre riešenie kvadratickej rovnice. Odtiaľ dostávame $\beta = (Tr(\alpha) \pm \sqrt{Tr(\alpha)^2 - 4})/2$, kde $\beta \in \mathbb{C}$.

Lemma 5.13. *Platí, že $\mathbb{Q}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$ je podokruh $\mathbb{H}$.*

Dôkaz. Keďže $\alpha \in \mathbb{H}$, tak $\mathbb{Q}[\alpha]$ je určite podmnožina $\mathbb{H}$. Stačí overiť, že je uzavretá na sčítanie a násobenie. Vezmime si $a_1 + b_1\alpha$, $a_2 + b_2\alpha \in \mathbb{Q}[\alpha]$. Potom platí:

- $(a_1 + b_1\alpha) + (a_2 + b_2\alpha) = (a_1 + a_2) + (b_1 + b_2)\alpha$,
- $(a_1 + b_1\alpha)(a_2 + b_2\alpha) = a_1a_2 + a_1b_2\alpha + b_1a_2\alpha + b_1b_2\alpha^2 = a_1a_2 + a_1b_2\alpha + b_1a_2\alpha + b_1b_2(Tr(\alpha)\alpha - 1) = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2 + b_1b_2Tr(\alpha))\alpha$.

Pri výpočte súčinu sme využili na vyjadrenie α^2 vzťah $\alpha^2 - Tr(\alpha)\alpha + 1 = 0$. Keďže $Tr(\alpha) \in \mathbb{Z}$, tak z výpočtov vidíme, že súčet aj súčin patrí do $\mathbb{Q}[\alpha]$, a teda sa jedná o podokruh.

□

Rovnako vieme, že pre $\beta \in \mathbb{C}$ platí, že $\mathbb{Q}[\beta] = \{a + b\beta \mid a, b \in \mathbb{Q}\}$ je okruh. Ľahko overíme, že zobrazenie $a + b\beta \to a + b\alpha$ dáva okruhový izomorfizmus $\mathbb{Q}[\beta] \simeq \mathbb{Q}[\alpha]$. Namiesto toho, aby sme ďalej skúmali generátor α, tak sa pozrieme bližšie práve na prvok β a následne využijeme tento izomorfizmus. Konkrétne sa pozrieme na kvadratické pole $\mathbb{Q}(\beta)$.

Keďže vieme, že $\beta = (Tr(\alpha) \pm \sqrt{Tr(\alpha)^2 - 4})/2$, tak označme $D = Tr(\alpha)^2 - 4$ diskriminant a ďalej nájdime také $D_1, D_2 \in \mathbb{Z}$, že platí $D = D_1D_2^2$ a navyše D_1 je bezštvorcové. Potom v skutočnosti platí $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D_1})$ a podľa definície 5.2 máme kvadratické pole. Ďalej ukážeme, že dané kvadratické pole je imaginárne. Budeme vychádzať z definície 5.3.

Lemma 5.14. *Ak $\beta = (Tr(\alpha) \pm \sqrt{Tr(\alpha)^2 - 4N(\alpha)})/2$, tak potom $\mathbb{Q}(\beta)$ je imaginárne kvadratické pole.*

Dôkaz. Ako sme už spomínali, tak $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{D})$ pre $D = Tr(\alpha)^2 - 4N(\alpha)$. Ukážeme, že $D < 0$. Na α sa môžeme pozerať ako na prvok $\mathbb{H}$, nech teda platí $\alpha = t + xi + yj + zk$. Potom $Tr(\alpha) = 2t$ a $N(\alpha) = t^2 + x^2 + y^2 + z^2$. Platí:

$$D = Tr(\alpha)^2 - 4N(\alpha) = (2t)^2 - 4(t^2 + x^2 + y^2 + z^2) = -4(x^2 + y^2 + z^2) \leq 0.$$

V prípade, že by malo platiť $D = 0$, tak nutne $x = y = z = 0$, čo znamená, že $\alpha \in \mathbb{R}$, konkrétne vďaka tvrdeniu 5.1 by bola $\alpha = \pm 1$. Na začiatku sme ale rovno predpokladali, že $\alpha \neq \pm 1$. Dokopy teda máme $D < 0$. Ak nájdeme $D_1, D_2 \in \mathbb{Z}$ také, že platí $D = D_1 D_2^2$ a navyše D_1 je bezštvorcové, tak nutne $D_1 < 0$. Z toho ale plynie, že $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{D_1})$ je imaginárne kvadratické pole.

□

Z predchádzajúceho dôkazu okrem iného vidíme aj to, že ak $D < 0$, tak potom $\beta \notin \mathbb{R}$. Teraz sa pozrieme na okruh celistvých prvkov v kvadratickom poli $\mathbb{Q}(\beta)$. Podľa definície 5.4 vieme, že β patrí do $\mathcal{O}_{\mathbb{Q}(\beta)}$, keďže je koreňom monického polynómu $x^2 - Tr(\alpha)x + 1 = 0$, kde $Tr(\alpha) \in \mathbb{Z}$. Ďalej budeme smerovať k tomu, aby sme ukázali, že β je v $\mathcal{O}_{\mathbb{Q}(\beta)}$ dokonca jednotkou.

Pre náš prvok $\beta \in \mathbb{Q}(\sqrt{D_1})$ platí, že β je koreňom monického polynómu $x^2 - tr(\beta)x + n(\beta)$. Toto platí pre každý prvok kvadratického poľa a overili sme to v predchádzajúcej sekcii. Zároveň ale pre β platí, že je koreňom monického polynómu $x^2 - Tr(\alpha)x + 1$. Z toho vidíme, že platí:

$$\beta^2 - tr(\beta)\beta + n(\beta) = 0 = \beta^2 - Tr(\alpha)\beta + 1 \Longrightarrow (Tr(\alpha) - tr(\beta))\beta = 1 - n(\beta).$$

Teraz buď platí $(Tr(\alpha) - tr(\beta)) = 0$, a teda z toho aj $1 - n(\beta) = 0$, čiže $n(\beta) = 1$. Alebo môžeme vyjadriť $\beta = (1 - n(\beta))/(Tr(\alpha) - tr(\beta))$. To je ale spor, pretože vieme, že $\beta \notin \mathbb{R}$.

Keďže pre β sme ukázali, že $n(\beta) = 1$, tak podľa tvrdenia 5.9 vieme, že β je jednotkou v okruhu celistvých prvkov $\mathcal{O}_{\mathbb{Q}(\beta)}$. Vyššie sme ešte v lemme 5.14 ukázali, že $\mathbb{Q}(\beta)$ je imaginárne kvadratické pole. Táto informácia pre nás bude teraz dôležitá z toho titulu, že pre imaginárne kvadratické polia vieme vo všeobecnosti popísať grupu jednotiek ich okruhu celistvých prvkov, ako sme ukázali vo vete 5.11.

Keďže β je jednotkou v $\mathcal{O}_{\mathbb{Q}(\beta)}$ pre imaginárne kvadratické pole $\mathbb{Q}(\beta)$, tak dostávame, že β je jedným z vymenovaných prvkov z vety 5.11. Dokonca platí, že β musí byť generátorom jednej z týchto spomenutých grúp jednotiek. Prepokladajme, že by β negenerovala celú grupu jednotiek. Potom vďaka izomorfizmu, o ktorom sme hovorili v úvode vieme, že ani α negeneruje celú grupu jednotiek v $\mathbb{Q}[\alpha]$. Keďže $\mathbb{Q}[\alpha] \subseteq \mathcal{O}$, tak grupa jednotiek v $\mathbb{Q}[\alpha]$ je podmnožina $\mathcal{O}^\times$. To by ale znamenalo, že $\langle\alpha\rangle \neq \mathcal{O}^\times$, čo je spor. Vieme teda, že β generuje $\{1, -1\}$ alebo $\{1, i, -1, -i\}$ alebo $\{\pm 1, (\pm 1 \pm \sqrt{-3})/2\}$. To znamená, že β má rád 2, 4 alebo 6. Vďaka izomorfizmu je potom aj $\langle\alpha\rangle$ grupa rádu 2, 4 alebo 6. Poznatky z tejto podkapitoly zhrnieme v nasledujúcej vete.

Veta 5.15. *Nech $\mathcal{O}$ je rád v kvaterniónovej algebre $B = \left(\frac{a,b}{\mathbb{Q}}\right)$, kde a, $b < 0$. Ak platí, že $\mathcal{O}^\times$ je netriviálna cyklická grupa, tak potom má rád 2, 4 alebo 6.*

5.3 Binárna dihedrálna grupa ako grupa jednotiek

Druhá možnosť je, že $\mathcal{O}^\times$ je binárna dihedrálna grupa rádu $4n$, kde $n > 1$. Zo sekcie 4.4 poznáme prezentáciu tejto grupy. Vďaka tomu vieme, že existujú $\alpha, \beta \in \mathcal{O}^\times$ také, že platí $\mathcal{O}^\times = \langle \alpha, \beta \mid \alpha^{2n} = 1, \beta^2 = \alpha^n, \beta^{-1}\alpha\beta = \alpha^{-1} \rangle$. Čiže $\mathcal{O}^\times$ má dva generátory, a to α rádu $2n$ a β rádu 4.

Pozrieme sa najprv na prvok β. Vieme, že je rádu 4, a teda $\beta^4 = 1$. Ukážeme, že potom nutne $\beta^2 = -1$. Na prvky α, β sa môžeme pozerať ako na prvky $\mathbb{H}$, a teda predpokladajme, že $\beta^2 = t + xi + yj + zk$. Platí:

$$1 = \beta^4 = (\beta^2)^2 = (t + xi + yj + zk)^2 = t^2 - x^2 - y^2 - z^2 + 2txi + 2tyj + 2tzk.$$

Potrebujeme teda, aby platilo:

$$t^2 - x^2 - y^2 - z^2 = 1 \qquad 2tx = 0 \qquad 2ty = 0 \qquad 2tz = 0.$$

Najprv predpokladajme, že $t = 0$. Následne z prvej rovnice dostávame podmienku $-x^2 - y^2 - z^2 = 1$, čo pre reálne x, y, z nie je možné. Z toho plynie, že $t \neq 0$. Potom ale zo zvyšných troch rovníc dostávame podmienky $x = y = z = 0$, čo po dosadení do prvej rovnice dáva $t^2 = 1$, z čoho vieme, že $t = 1$ alebo $t = -1$. Keďže $\beta^2 = t$, tak potom $\beta^2 = t = -1$, keďže β má rád až 4 a nie 2.

Teraz sa pozrieme na prvok α. Vieme, že α má rád $2n$, a teda môžeme povedať, že v $\mathcal{O}^\times$ samotný prvok α generuje cyklickú grupu rádu $2n$. Ako sme ukázali v predchádzajúcej sekcii 5.2, jediné cyklické grupy, ktoré prichádzajú do úvahy, sú rádu 2, 4 alebo 6. Pričom, ak by α mala rád 2, tak sa potom nejedná o binárnu dihedrálnu grupu, čiže túto možnosť môžeme vylúčiť. Ostali dve možnosti, ktoré postupne rozoberieme.

Prvok α má rád 4

Keď sa pozrieme na prezentáciu danej binárnej dihedrálnej grupy $\mathcal{O}^\times = \langle \alpha, \beta \mid \alpha^{2n} = 1, \beta^2 = \alpha^n, \beta^{-1}\alpha\beta = \alpha^{-1} \rangle$, tak z toho, že α má rád 4 vidíme, že $n = 2$. Potom z druhej podmienky spolu s $\beta^2 = -1$, dostávame $\alpha^2 = \beta^2 = -1$.

Vieme, že pôvodne bol $\mathcal{O}$ rád v algebre $B = \left(\frac{a,b}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$. Zadefinujme novú kvaterniónovú algebru $B' = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$. Potom platí $B' = \left(\frac{-1,-1}{\mathbb{Q}}\right)$. Najprv dokážeme poslednú rovnosť. Vieme, že $\{1, \alpha, \beta, \alpha\beta\}$ je báza a platí $\alpha^2 = -1$, $\beta^2 = -1$. Ostáva ukázať, že $\alpha\beta = -\beta\alpha$. Z prezentácie $\mathcal{O}^\times$ vieme, že platí rovnosť $\beta^{-1}\alpha\beta = \alpha^{-1}$, ktorá sa dá upraviť ako $\alpha\beta = \beta\alpha^{-1}$. Zároveň z podmienky $\alpha^2 = -1$ plynie $\alpha = -\alpha^{-1}$. Dokopy dostávame práve požadovanú rovnosť $\alpha\beta = \beta\alpha^{-1} = -\beta\alpha$.

Vieme, že B aj B' majú, ako vektorové priestory, rovnakú dimenziu rovnú 4. Keďže α, $\beta \in B$, tak platí $\mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta \subseteq \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$. Z rovností dimenzií potom plynie, že sú si dané vektorové priestory rovné a dokopy:

$$B' = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij = \left(\frac{a,b}{\mathbb{Q}}\right) = B.$$

Odteraz pracujeme s tým, že $\mathcal{O}^\times \subseteq \mathcal{O} \subseteq \left(\frac{-1,-1}{\mathbb{Q}}\right)$.

Keďže $\mathcal{O}$ je $\mathbb{Z}$-rád a $\alpha,\ \beta \in \mathcal{O}$, tak platí, že $\mathcal{O}$ obsahuje rád generovaný α a β. Konkrétne môžeme písať $\mathbb{Z}+\mathbb{Z}\alpha+\mathbb{Z}\beta+\mathbb{Z}\alpha\beta \subseteq \mathcal{O}$. Uvedomme si, že v tom prípade je $\mathbb{Z}+\mathbb{Z}\alpha+\mathbb{Z}\beta+\mathbb{Z}\alpha\beta$ rád v $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ a platí $\alpha^2=\beta^2=-1$, $\alpha\beta=-\beta\alpha$. To znamená, že sa jedná o Lipschitzov rád z definície 3.9, ktorý sme rozoberali v sekcii 3.2 a 3.3. Podľa tvrdenia 3.16 jediný rád, ktorý vlastne obsahuje Lipschitzov rád je Hurwitzov rád z definície 3.13.

Vychádzajúc z toho, že $\mathbb{Z}+\mathbb{Z}\alpha+\mathbb{Z}\beta+\mathbb{Z}\alpha\beta \subseteq \mathcal{O}$, tak buď nastáva rovnosť a $\mathcal{O}$ je samotný Lipschitzov rád, alebo potom práve spomínaný Hurwitzov rád. Ak by bol $\mathcal{O}$ Lipschitzov rád, tak podľa dôsledku 3.12 máme $\mathcal{O}^\times = Q_8$. Vieme, že Q_8 je v hamiltonovských kvaterniónoch $\{\pm 1, \pm i, \pm j, \pm k\}$, čo vieme iným spôsobom zapísať ako $\langle i, j \mid i^4=1, j^2=i^2, j^{-1}ij=i^{-1}\rangle$. Posledná podmienka plynie zo vzťahu $ij=-ji$. To znamená, že $\mathcal{O}^\times = Q_8$ je binárna dihedrálna grupa Dic_2, tak, ako sme požadovali. Tento prípad teda vyhovuje.

Teraz uvažujme, že by bol $\mathcal{O}$ Hurwitzov rád. Podľa tvrdenia 3.15 je grupa jednotiek v Hurwitzovom ráde $\{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}$. To sme však následne v 4. kapitole ukázali, že je binárna tetrahedrálna grupa z definície 4.9. My však v tejto sekcii požadujeme, aby $\mathcal{O}^\times$ bola binárna dihedrálna grupa. Tým pádom táto možnosť nevyhovuje.

Ukázali sme, že v prípade, ak má α rád 4, tak je možné, aby $\mathcal{O}^\times$ bola binárna dihedrálna grupa, pričom to bude Q_8.

Prvok α má rád 6

Potom prezentácia vyzerá ako $\mathcal{O}^\times = \langle \alpha, \beta \mid \alpha^6=1, \beta^2=\alpha^3, \beta^{-1}\alpha\beta=\alpha^{-1}\rangle$. Išlo by teda o binárnu dihedrálnu grupu rádu 12. Poďme sa pozrieť, či a kedy tento prípad môže nastať. Ako sme už vysvetlili v predchádzajúcej sekcii, tak $\mathbb{Q}[\alpha]$ je izomorfné $\mathbb{Q}[\gamma]$, kde $\gamma \in \mathbb{C}$ je nejaká jednotka spomenutá vo vete 5.11. Tento izomorfizmus je daný vzťahom $a+b\gamma \longrightarrow a+b\alpha$, a teda sa v ňom γ zobrazí na α. Keďže α má rád 6, tak nutne aj γ bude mať rád 6, a teda $\gamma=-\omega$ alebo $\gamma=-\omega^2$, kde $\omega=(-1+\sqrt{-3})/2$. Vieme teda, že v danom izomorfizme α odpovedá niektorému z prvkov $-\omega$, $-\omega^2$.

Pôvodne platilo $\mathcal{O} \subseteq B = \left(\frac{a,b}{\mathbb{Q}}\right) = \mathbb{Q}+\mathbb{Q}i+\mathbb{Q}j+\mathbb{Q}ij$. Vieme, že stále $\beta^2=-1$, takže zadefinujeme novú kvaterniónovú algebru ako $B' = \left(\frac{-3,-1}{\mathbb{Q}}\right) = \mathbb{Q}+\mathbb{Q}\sqrt{-3}+\mathbb{Q}\beta+\mathbb{Q}\sqrt{-3}\beta$. Následne vďaka izomorfizmu popísanému v predchádzajúcom odseku dostávame $B' = \mathbb{Q}+\mathbb{Q}\sqrt{-3}+\mathbb{Q}\beta+\mathbb{Q}\sqrt{-3}\beta \simeq \mathbb{Q}+\mathbb{Q}\alpha+\mathbb{Q}\beta+\mathbb{Q}\alpha\beta$.

Zároveň $\alpha, \beta \in \mathcal{O}^\times$, čiže platí $\mathbb{Q}+\mathbb{Q}\alpha+\mathbb{Q}\beta+\mathbb{Q}\alpha\beta \subseteq \mathbb{Q}+\mathbb{Q}i+\mathbb{Q}j+\mathbb{Q}ij$. Ale opäť, keďže ako vektorové priestory majú rovnakú dimenziu 4, tak sú si rovné. Z toho dokopy máme:

$$\begin{aligned} B = \left(\frac{a,b}{\mathbb{Q}}\right) &= \mathbb{Q}+\mathbb{Q}i+\mathbb{Q}j+\mathbb{Q}ij \simeq \mathbb{Q}+\mathbb{Q}\alpha+\mathbb{Q}\beta+\mathbb{Q}\alpha\beta \\ &\simeq \mathbb{Q}+\mathbb{Q}\sqrt{-3}+\mathbb{Q}\beta+\mathbb{Q}\sqrt{-3}\beta = \left(\frac{-3,-1}{\mathbb{Q}}\right) = B'. \end{aligned}$$

Keď sa na rád $\mathcal{O}$ budeme pozerať vzhľadom k danému izomorfizmu, ako na rád v kvaterniónovej algebre $\left(\frac{-3,-1}{\mathbb{Q}}\right)$, tak obsahuje prvky β a ω. Prvok ω obsahuje preto, lebo sa naňho zobrazil prvok α. To ale znamená, že $\mathbb{Z}$-rád $\mathcal{O}$ obsahuje rád $\mathbb{Z}+\mathbb{Z}\omega+\mathbb{Z}\beta+\mathbb{Z}\omega\beta$.

To je však presne rád, ktorým sme sa zaoberali na konci 3. kapitoly, akurát sme v značení používali j, ktoré teraz predstavuje β. Ako sme sľúbili, teraz uvidíme dôvod, prečo sme si v tretej kapitole vybrali práve tento rád. V tvrdení 3.20 sme dokázali, že je maximálny. Z toho priamo plynie, že $\mathcal{O} \simeq \mathbb{Z} + \mathbb{Z}\omega + \mathbb{Z}\beta + \mathbb{Z}\omega\beta$.

Keď sme už určili ako vyzerá rád $\mathcal{O}$, tak posledným krokom je overiť, či grupa jednotiek $\mathcal{O}^\times$ bude v takomto prípade binárna dihedrálna grupa. V tvrdení 3.21 sme ukázali, že rád $\mathbb{Z} + \mathbb{Z}\omega + \mathbb{Z}\beta + \mathbb{Z}\omega\beta$ má ako grupu jednotiek $\mathcal{O}^\times = \{\pm 1, \pm\beta, \pm\omega, \pm\omega^2, \pm\omega\beta, \pm\omega^2\beta\}$. Táto grupa naozaj je binárna dihedrálna grupa rádu 6, pretože ju môžeme vyjadriť ako $\mathcal{O}^\times = \langle -\omega, \beta \mid (-\omega)^6 = 1, \beta^2 = (-\omega)^3, \beta^{-1}(-\omega)\beta = (-\omega)^{-1}\rangle$. Vidíme, že táto možnosť môže nastať, a teda ak má α rád 6, tak je možné, aby $\mathcal{O}^\times$ bola binárna dihedrálna grupa rádu 12. Opäť zhrnieme, čo sme zistili v nasledujúcej vete.

Veta 5.16. *Nech $\mathcal{O}$ je rád v kvaterniónovej algebre $B = \left(\frac{a,b}{\mathbb{Q}}\right)$, kde a, $b < 0$. Ak platí, že $\mathcal{O}^\times$ je binárna dihedrálna grupa, tak potom má rád 8 alebo 12.*

5.4 Binárna tetrahedrálna, oktahedrálna alebo ikosahedrálna grupa ako grupa jednotiek

Ostávajú možnosti, že by $\mathcal{O}^\times$ bola binárna tetrahedrálna, binárna oktahedrálna alebo binárna ikosahedrálna grupa. Tieto prípady vyriešime spoločne. Pozrieme sa na vyjadrenie týchto grúp pomocou kvaterniónov v definíciách 4.9, 4.12 a 4.15. Môžeme vidieť, že každá z nich obsahuje ako podgrupu $\{\pm 1, \pm i, \pm j, \pm k\}$. To vidíme, že je podľa definície 3.10 kvaterniónová grupa Q_8.

Ako sme už v predchádzajúcej sekcii ukázali, kvaterniónová grupa Q_8 sa dá zapísať ako $\langle i, j \mid i^4 = 1, j^2 = i^2, j^{-1}ij = i^{-1}\rangle$, a teda ide o binárnu dihedrálnu grupu rádu 8. Takže sme práve ukázali, že ak bude $\mathcal{O}^\times$ binárna tetrahedrálna, binárna oktahedrálna alebo binárna ikosahedrálna grupa, tak stále bude obsahovať ako podgrupu práve binárne dihedrálnu grupu.

Následne môžeme aplikovať postup z predchádzajúcej kapitoly a jediný nový prípad, ktorý dostávame je, že $\mathcal{O}^\times$ bude binárna tetrahedrálna grupa rádu 24, ktorú získame ako grupu jednotiek Hurwitzovho rádu.

Týmto sme sa prepracovali k tomu, čo sme si dali ako hlavný cieľ a podrobne sme dokončili klasifikáciu grúp jednotiek v rádoch v hamiltonovských kvaterniónoch. Tento hlavný výsledok zhrnieme v nasledujúcej vete.

Veta 5.17 (klasifikácia grúp jednotiek v rádoch v hamiltonovských kvaterniónoch)**.** *Nech $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ je kvaterniónová algebra, kde a, $b < 0$ a $\mathcal{O} \subseteq B$ je rád. Potom grupa jednotiek $\mathcal{O}^\times$ je jedného z nasledujúcich typov:*

- *cyklická grupa rádu 2, 4 alebo 6,*
- *kvaterniónová grupa Q_8 rádu 8,*
- *binárna dihedrálna grupa rádu 12,*
- *binárna tetrahedrálna grupa rádu 24.*

Zoznam použitej literatúry

[1] John C. Baez. From the Icosahedron to E8 [online]. https://arxiv.org/pdf/1712.06436.pdf.

[2] Hong Thien An Bui. Classifying the finite subgroups of $SO(3)$ [online]. http://math.uchicago.edu/~may/REU2020/REUPapers/Bui,An.pdf.

[3] Keith Conrad. Dihedral groups [online]. https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral.pdf.

[4] Keith Conrad. Factoring in quadratic fields [online]. https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf.

[5] Keith Conrad. Quaternion algebras [online]. https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf.

[6] Harold S. M. Coxeter and William O. J. Moser. *Generators and Relations for Discrete Groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 2. Folge. Springer Berlin Heidelberg, 2013.

[7] Peter R. Cromwell. *Polyhedra*. Cambridge University Press, Cambridge, 1997.

[8] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[9] Tsit-Yuen Lam. *A First Course in Noncommutative Rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.

[10] John Stillwell. *The four pillars of geometry*. New York, NY: Springer, 2005.

[11] John Voight. Quaternion algebras [online]. https://math.dartmouth.edu/~jvoight/quat-book.pdf.